EUROPEAN
COMMISSION

Brussels, 8.7.2014
SWD(2014) 225 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT AND THE COUNCIL**
**Better situational awareness by enhanced cooperation across maritime surveillance
authorities: next steps within the Common Information Sharing Environment for the
EU maritime domain**

{COM(2014) 451 final}
{SWD(2014) 224 final}

EN   **EN**

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain

Table of contents

Table of Figures and Tables

1.   EXECUTIVE SUMMARY SHEET

Impact assessment in support of a Communication on a Common information sharing environment for the EU maritime domain

A. Need for action

Why? What is the problem being addressed?

The current information exchange between maritime surveillance authorities in the EU is suboptimal and leads to efficiency losses, duplication of data collection efforts and unnecessary operational costs. The link that would require further development, building on existing solutions and developments, relates to common standards which would allow for the interoperability of sectorial systems and machine readable information services. This would further enhance the possibilities for these authorities to have getting access to all the information necessary for their operative work. The main causes are real or perceived legal limitations, technical and cultural barriers which are preventing the desired information exchange.

Under the baseline scenario, the situation is expected to improve also in the future due to enhanced co-operation between different maritime surveillance functions (maritime safety and security, border control, customs, general law enforcement, fisheries control, environmental control and defence) but is expected to remain suboptimal in the absence of an interoperability framework at EU level which would allow authorities to communicate and exchange information services more effectively. The relevant stakeholders are maritime surveillance authorities at national level (national coastguards etc.) and at EU level (FRONTEX, EMSA, EFCA, EDA, etc.).

What is this initiative expected to achieve?

The purpose of this initiative is to ensure that maritime surveillance information and services collected by one maritime sector and considered necessary/useful for the activities of other maritime sectors or functions can be efficiently shared with those sectors. Of particular importance is the objective to achieve enhanced exchange of information services between civilian and military authorities. This objective will have to be achieved through the removal of real or perceived legal and cultural limitations and through the use of an interoperability standard which would allow for this information exchange, based on existing models.

Better exchange of information services are expected to lead to less duplication of data collection efforts, more cost efficient maritime surveillance operations and a better maritime surveillance awareness in EU waters.

What is the value added of action at the EU level?

Information exchange between maritime surveillance authorities/functions are of a transnational nature since it normally entails co-operation first and foremost at regional or sea basin level. Moreover, rules and conditions for transnational sharing of maritime surveillance information between authorities of a same sector are already regulated at EU level and involve EU agencies.

B. Solutions

What legislative and non-legislative policy options have been considered? Is there a preferred choice or not? Why?

The impact assessment considers 3 options with different sub-options. Several options (including one to review all existing information exchange systems) were discarded from the beginning as it would be counterproductive to the overall objectives of the initiative as making past work obsolete.

The three options are 1) the baseline scenario (no further action at EU level) 2) voluntary measures,(including sub-options for a Communication by the Commission, the adoption of a handbook and best practices through a Recommendation and a joint undertaking) and 3) binding measures (including sub-options for revisions of existing sector legislation at EU level, an EU Regulation for a Common Information Sharing Environment, and a technical Regulation on interoperability standards).

The preferred option is a mix of several sub-options, including the adoption of a Commission Communication, a handbook with best practices adopted through a Recommendation as well as revisions of sector legislation to remove unjustified legal limitations.

Who supports which option?

All input from the stakeholder consultation and a specific survey among the Member States as well as other preparatory actions (in particular pilot projects involving Member States representatives) demonstrate a firm support among stakeholders for EU action on this initiative. Stakeholders are however more divided as to the choice between binding versus non-binding options. The overall conclusion of stakeholders seem to be that binding measures are necessary but should be limited to the removal of any remaining unjustified legal limitations and technical barriers whereas non-binding measures through guidance should tackle cultural barriers at national level. This conclusion is in line with the conclusion of the impact assessment.

C. Impacts of the preferred option

What are the benefits of the preferred option?

The overall potential impact (benefit) of CISE is estimated to range between 1.6 billion € and 4.2 billion € over ten years as from the moment CISE is in place.

These potential benefits of CISE as quantified in economic terms have social and environmental relevance as they stem from increased success in reducing goods being smuggled into the EU, oil polluting the sea, illegal unregulated and unreported fisheries, accidents at sea, irregular immigration, smuggling of small arms/light weapons, piracy and most importantly, succeeding in saving more lives at sea.

The mix of preferred policy options mentioned in the preceding section is estimated to reap about 80% of the above mentioned overall economic impact (benefit).

What are the costs of the preferred option?

The total cost over 10 years for the preferred option is estimated at 133M€. EU central cost amounts to 26 M€ and Member States cost amounts to 107 M€ over 10 years.

The cost of implementing CISE depends to a large extent on how each Member State may want to organise itself internally to connect to the environment, on the number of information services that will be provided in the environment and on the large variety of existing and planned IT systems. It is proposed not to impose any organisational structure to the Member States and let Member States connect to CISE their IT systems per sectorial functions. It is estimated that the above mentioned cost are necessary to reach the preferred policy mix reaping about 80% of the above mentioned overall economic impact (benefit).

How will businesses, SMEs and micro-enterprises be affected?

This initiative concerns only maritime surveillance authorities in the EU. Private companies such as SMEs and micro enterprises are not directly affected by this proposal. They will however benefit from a better business environment as enhanced maritime surveillance will ensure cleaner, safer and more secure seas as fundamental conditions to fostering blue growth, sustainable development and security of the EU maritime domain.

Further, CISE provides business opportunities as new information services and technologies will be developed by businesses for the said public authorities.

Will there be significant impacts on national budgets and administrations?

No. Cost per Member State amounts to between 2 M€ and 4 M€ for the ten year budgeting period, to adhere to a common information sharing environment. No other costs are envisaged.

Will there be other significant impacts?

The initiative will hopefully lead to a smarter use of existing resources and funds and simplify co-operation between maritime surveillance authorities in accordance with the refit initiative of the Commission. It is not expected to have any negative impacts on fundamental rights of citizens, competitiveness of private companies or international relations.

It is expected that enhancing knowledge and improving maritime situational awareness could potentially lead to the reduction of threats and risks by 30% on average, while this effect will of course not be uniform over the type of risk and the different maritime areas of European interest.

D. Follow up

When will the policy be reviewed?
The development of this policy initiative will be reviewed after 4 years. Progress will be discussed regularly within the framework of a Member State expert group.

2. INTRODUCTION AND SCENE SETTER

The purpose of this impact assessment is to examine to what extent EU action is necessary to enhance the exchange of maritime surveillance information services[1] between the maritime surveillance authorities[2] in the EU.

The creation of a Common Information Sharing Environment (hereinafter CISE) for the EU maritime domain[3] has been discussed in a EU context since 2007[4] and has so far been the subject matter of two Communications of the Commission in 2009 and 2010[5]. These discussions have already produced some success stories and gradually lead to enhanced information exchange, in particular between civilian surveillance authorities.[6] However, further improvements seem feasible to enhance exchange not only between civilian maritime surveillance authorities, but in particular information exchange between civilian and military authorities.

This work should be seen against the background of an increasing number of situations and events which can negatively affect the EU maritime domain today and within the next 15 years. In short, the EU maritime domain is exposed to various and growing man-made, accidental and natural threats and risks[7].

These threats and risks can partially be explained by the fact that trade with third countries and movements of persons across borders have increased steadily in recent years and we can expect that these movements will continue to increase in the future.

---

[1] For the purpose of this impact assessment the use of the term "data" usually refers to raw or unprocessed data which are formatted in a special way. The term "information" is usually used when data has been treated and taken a certain meaning.

[2] Maritime surveillance authorities are those civilian and military authorities who in one way or the other are involved in or have the responsibility to carry out surveillance activities not only in waters under the sovereignty and jurisdiction of EU Member States but also in any international waters of interest to the EU, such as in the Gulf of Aden where the Operation Atalanta has been carried out. These authorities can be either national authorities (such as the national coastguard) or EU level authorities (such as EFCA, FRONTEX, EMSA).

[3] There is not yet an agreed definition of this term, but the EU Maritime domain is commonly referred to as the waters under the sovereignty and jurisdiction of the EU Member States (in most cases up until a 200 nautical miles Exclusive economic Zone) under the Law of the Sea Convention (UNCLOS). The concept also include maritime surveillance activities carried out in other maritime areas where the EU has a security interest (such as the gulf of Aden outside the horn of Africa to protect our merchant vessels from piracy attacks) and all the maritime-related activities carried out by EU bodies or Member States under civil and military authority in accordance with our obligations under international and EU law (such as search and rescue operations or fisheries control operations).

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - An Integrated Maritime Policy for the European Union {COM(2007) 574 final)} - 10 Oct 2007

[5] Communication from the Commission to the Council, the European Parliament, the European economic and social Committee and the Committee of the regions: "Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain" COM(2009)538 final – 15.10.2009, and the Communication from the Commission to the Council, the European Parliament, the European economic and social Committee and the Committee of the regions, on a draft roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain COM (2010)584 final – 20.10.2010.

[6] For example, the Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC envisages sharing of data collected through a single point of contact ("single window") to several functions (maritime safety and security, border control, customs and health) based on their legal requirements.

[7] See inter alia risk assessment study in the consultancy report in support of this impact assessment.

A significant proportion of entries to the EU are seaborne. For example, 74% of the EU's external trade is carried by sea[8]. Increased number of threats therefore risks entering the EU by sea and may be spread through Member States within a very short period of time.

Detecting, checking and thwarting those threats - from post 9/11 terrorism, influx of illegal drugs and arms, illegal immigration to customs fraud and environmental damages or even from unintended accidents or natural events - are crucial to ensure the fundamental conditions for the safety, the security and prosperity of the EU and its population.

It falls under the responsibility of the maritime surveillance authorities of the Member States to face those threats. Their responsibility is not only to carry out operations at sea, but also inter alia to ensure the effective understanding of all activities carried out at sea and events occurred at sea that could impact the security, safety, economy or environment of the European Union and its Member States, this is commonly referred to as "maritime domain awareness"[9]. Seven different functions are relevant in this context: (1) maritime safety (including search and rescue), maritime security and prevention of pollution caused by ships, (2) fisheries control, (3) marine pollution preparedness and response, marine environment protection (4) customs, (5) border control, (6) general law enforcement and (7) defence.[10]

The increased maritime surveillance and control needs which are required to face these threats put an additional burden on the maritime surveillance authorities. Increased control activities cost money however and putting additional funds into maritime surveillance is not evident in times of financial crisis, when many national and EU authorities are reducing their costs. This means that maritime surveillance authorities of the EU Member States are obliged to become more effective and cost efficient when carrying out their duties.

There is in other words a need to enhance co-operation with other maritime surveillance authorities of other functions at national level and/or of other Member States. Such co-operation would inter alia strive for more effective and coordinated actions at sea, create synergies, mutual knowledge and sharing of experience/actions at sea. Information services are needed to foster such co-operation. The subject matter for this impact assessment is to a large extent about better regulations and making better use of existing solutions in in the area of maritime surveillance along the spirit of the REFIT initiative of the Commission[11] rather than creating new rules.

Many Member States have already or are in the process of setting up national initiatives to this end and initiatives have been launched at EU level. One example of EU level initiatives is the 2009 initiative for the coast guard functions cooperation through the Forum of the Heads of the Coast Guard Functions of the European Union and Schengen associated countries (so

---

[8]   Communication from the Commission: Ports, an engine for growth – COM(2013) 295 final - 23.05.2013

[9]   As referred to the equivalent definition of "maritime situational awareness" in the Communication from the Commission to the Council, the European Parliament, the European economic and social Committee and the Committee of the regions: "Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain" COM(2009)538 final – 15.10.2009 and to the definition of "Maritime Domain Awareness" by the International Maritime Organization in Amendments to the International Aeronautical and Maritime Search and Rescue (IAMSAR) Manual (24.05.2010).

[10]   This is a relatively simplified picture for illustration purposes. The definition of the tasks attached to these functions is independent from how maritime surveillance functions are organised at national level which can vary to a great extent from one Member State to the next.

[11]   See communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and Committee of the regions – Strengthening the foundations of smart Regulation – Improving evaluation - COM (2013) 686 final) of 2 October 2013.

called "European Coast Guard Functions Forum")[12]. A Commission study looking into the feasibility of improved co-ordination between bodies carrying out coast guard functions at European level is currently on-going. The very preliminary results of this study are that suboptimal information sharing is a general obstacle to enhanced collaboration. Suggestions for improvement include simplified procedures for the adoption of analytical standards and procedures, the development of tools to report on the information shared as well as the encouragement of automatic and cross sector information sharing. Another example is the number of Service Level Agreements on information exchange which has been concluded between various EU agencies[13].

These initiatives for a more integrated and co-operative approach to the surveillance of our seas, coasts and oceans have inter alia been inspired by the development of the Integrated Maritime Policy (IMP) of the EU[14]. Its main aim is to increase co-ordination between various sectorial maritime policies within the EU to enhance their effectiveness and cost efficiency. The Blue book on the IMP[15] has identified work towards more integrated maritime surveillance activities supported inter alia by the creation of a Common Information Sharing Environment (CISE) as an important step in this direction.

CISE is also a part of wider Commission objectives expressed in its 'Europe 2020' strategy for smart, sustainable and inclusive growth. By helping to ensuring safe, secure and clean seas, CISE can support the fundamental conditions for sustainable (blue) growth.

CISE also contributes to the 'Digital Agenda for Europe' and to the ISA Programme, which supports the delivery of European public services by fostering cross border and cross sector interoperability, and thus contributes to the European single digital market as well as to computer literacy.

CISE further fosters the 'Innovation Union' both in the public and private sectors through the development of new technologies and by engaging in new ways of cooperation between about 400 relevant public authorities within the EU/EEA, saving time and money.

As a tool helping public authorities to optimise the deployment of their assets, CISE could also contribute to the 'Resource-efficiency' flagship initiative under the Europe 2020 strategy that supports the shift towards a resource-efficient, low-carbon economy for sustainable growth.

In particular to achieve safe, secure and clean oceans through enhanced management and control. It is targeting the control aspects of the management of the sea and should therefore be seen as complementary to a number of existing measures within this area, including the Marine Strategy Framework Directive, the CFP Regulation, the Reporting Formalities Directive, the EUROSUR Regulation, as well as other non-legislative initiatives such as EMODNET, innovation in the blue economy, and blue growth. The main idea of CISE is to ensure that the systems collecting data under any such initiatives will become interoperable, thus allowing for example data collected under EMODNET to be available to maritime surveillance authorities of other sectors when needed.

---

[12]   http://www.ecgff.eu/
[13]   E.g. Service Level Agreements concluded between EMSA and FRONTEX, EMSA and EFCA, and EFCA and FRONTEX (see section 4.4.1)
[14]   See footnote 4
[15]   See footnote 4

Member States, Council and other stakeholders have so far been very supportive of these initiatives.[16]

3. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

3.1. Identification

The objective of this impact assessment is to provide an analysis of the options for EU action to implement CISE. The agenda planning reference is 2012/MARE/002.

This impact assessment aims at:

• Analysing the need for EU action, and

• Determining the most suitable option and delivery instrument for this action.

3.2. Impact assessment steering group

An impact assessment steering group was created in June 2012 and met 9 times between 20th June 2012 and 24 October 2013. The Impact Assessment Steering Group was composed of Legal Service (SJ), Secretariat-General (SG), Directorate-General for Mobility and Transports (MOVE), Directorate-General for Home Affairs (HOME), Directorate-General for Justice (JUST), Directorate-General for Taxation and Customs Union (TAXUD), Directorate-General for Humanitarian Aid and civil protection (ECHO), Directorate –General for Enterprise and Industry (ENTR), Directorate-General for Communication Networks, Content and Technology (CNECT), Directorate-General for Informatics (DIGIT), European Anti-Fraud Office (OLAF), Joint Research Centre (JRC) and European External Action Service (EEAS).

3.3. Consultation and expertise

Stakeholders' consultations referred to in this document took place in several fora which are listed below.

3.3.1. Public consultation

On 14 June 2013, a three-month public consultation was launched in support of the present impact assessment. The consultation ended on 14 September 2013. A total of 33 responses were received, among which 24 responses were made on behalf of organisations/administrations. The overall result of this consultation was as follows:

• Overall recognition that co-operation and information exchange between maritime surveillance authorities of different sectors is unsatisfactory and could be improved;

---

[16] Declaration of the European Ministers responsible for the Integrated Maritime Policy and the European Commission, on a Marine and Maritime Agenda for growth and jobs "The Limassol Declaration" – 07.10.2012- para 22 - http://ec.europa.eu/maritimeaffairs/policy/documents/limassol_en.pdf; GAERC Conclusions on Integrated Maritime Policy and Maritime Surveillance (25.06.2013, para 6), GAERC conclusions on the Marine and Maritime Agenda for Growth and jobs (11.12.2012, para 9), ENVC Conclusions on the Integrated Maritime Policy (19.11.2011, para 14), GAERC Conclusions on Integration of Maritime Surveillance (17.11.2009) and GAERC Conclusions on Integrated Maritime policy and Maritime Surveillance (8.12.2008, p 45 para 5); European Parliament resolution of 21 October 2010 on Integrated Maritime Policy - Evaluation of progress made and new challenges (2010/2040(INI) (para 36) - http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0386&language=EN

- Overall recognition that improved co-operation and information exchange could help reduce cost and improve efficiency of surveillance activities;

- Overall belief that efforts need to be stepped up at EU level to address possible legal limitations and, technical and cultural barriers and that these efforts have to be achieved through binding measures where necessary to address certain limitations or barriers.

Further details regarding the results of this consultation can be found in Annex 1.

3.3.2. Other consultations

In addition, a specific survey targeting Member States experts on maritime surveillance took place between May 2013 and June 2013. This survey was focusing on cost aspects, possible limitations to information exchange and the potential benefits of enhanced information exchange. The result of this Member State survey was as follows:

- Overall difficulty for Member States to provide anything more than indicative estimations of what the cost aspects of maritime surveillance activities could be, but nevertheless an expectation that increased information exchange could lead to less duplication of efforts and thus reduced cost;

- Confirmation that there are existing or perceived legal, technical and cultural limitations which impede optimal information exchange between maritime surveillance authorities. The perceived impact of these limitations varies to a large extent from one Member State to the next.

- Confirmation that enhanced information could have moderate to significant benefits for maritime surveillance activities. Potential benefits include better response capability, better surveillance outcomes, cost savings for information gathering and better use of assets.

Further details regarding the results of this consultation can be found in Annex 2.

3.3.3. Dialogues and consultations with other Institutions, other Services and Member States

The Council of the European Union, the European Parliament and the European Economic and Social Committee have provided support to the CISE project through inter alia the following initiatives:

In 2012, European Ministers called for the CISE project to be operational by 2020 in the so called "Limassol declaration"[17].

Since 2008, the Council have issued a number of Council conclusions in support of the CISE project[18].

---

[17]   Declaration of the European Ministers responsible for the Integrated Maritime Policy and the European Commission, on a Marine and Maritime Agenda for growth and jobs "The Limassol Declaration" – 07.10.2012, see para 21: *"We reaffirm that growth can be boosted by coherent and effective public policy that sets out the conditions necessary for the full development of the blue economy. It should reduce administrative and regulatory burdens and remove bottlenecks for innovation and investment. We therefore call for involved parties to: (…) Support the integration of maritime surveillance towards an active operational Common Information Sharing Environment for the EU maritime domain by 2020, as an effective and cost-efficient way of safeguarding EU interests"*
http://ec.europa.eu/maritimeaffairs/policy/documents/limassol_en.pdf.

[18]   See inter alia GAERC Conclusions on Integrated Maritime Policy and Maritime Surveillance (25.06.2013, para 6), GAERC conclusions on the Marine and Maritime Agenda for Growth and jobs

In 2010 and 2012, the European Parliament called on the European Union to create a common information sharing environment in a Resolution on the Integrated Maritime Policy of the EU[19] and to invest meaningfully in further developing the CISE framework, in a report on the maritime dimension of the Common Security and Defence Policy[20].

European Economic and Social Committee issued a favourable Opinion[21] on the 2010 Communication by the Commission on CISE referred to above.

The European Data Protection Supervisor will be consulted on the CISE project before the adoption of the policy package.

Maritime surveillance authorities were closely involved in the process up to now:

- A specific Member State expert sub-group on integrated maritime surveillance was established in September 2009 and has since then met 11 times. The purpose of this expert group is to discuss and provide political guidance on maritime surveillance in general and on the CISE project in particular. This group involves representatives from all EU and EEA Member States. All relevant EU Agencies are also invited to participate in this work: the European Maritime Safety Agency (EMSA) (transport), the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the EU (FRONTEX), the European Environmental Agency (EEA), European Police Office (EUROPOL), the European Fisheries Control Agency (EFCA), the European Satellite Centre (EUSC) and the European Defence Agency (EDA).

- A specific Technical Advisory Group (TAG) on integrated of maritime surveillance was established in November 2010 and has since then met 15 times. The purpose of this group is to obtain technical guidance from the different functions on the CISE project. TAG is composed of national or EU[22] experts representing the seven sectorial functions, as well as representatives from all the above mentioned European agencies. Each TAG member has been nominated by its sectorial function and has the task to liaise with counterparts from all involved countries inside his/her sector, to ensure as wide representation as possible.

- Further, two large scale CISE pilot projects ('BLUEMASSMED'[23] and 'MARSUNO'[24]) were launched in 2010 and finalised in 2012. The final reports of

---

(11.12.2012, para 8), ENVC Conclusions on the Integrated Maritime Policy (19.11.2011, para 13), GAERC Conclusions on Integration of Maritime Surveillance: "towards the integration of Maritime Surveillance: a Common Information and Sharing Environment for the EU maritime domain (23.05.2011), GAERC Conclusions on Integrated Maritime Policy (14.06.2010, para 11), GAERC Conclusions on Integration of Maritime Surveillance (17.11.2009) and GAERC Conclusions on Integrated Maritime policy and Maritime Surveillance (8.12.2008, p 45 para 5 and 6)

[19] European Parliament resolution of 21 October 2010 on Integrated Maritime Policy - Evaluation of progress made and new challenges (2010/2040(INI) (para 31-36)
http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0386&language=EN

[20] Parliament report on the maritime dimension of the Common Security and Defence Policy (2012/2318(INI)) - Committee on Foreign Affairs
http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/2318%28INI%29&l=en

[21] Opinion of the European Economic and Social Committee on the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Towards the integration of maritime surveillance: a common information sharing environment for the EU maritime domain (14.07.2010)
http://www.eesc.europa.eu/?i=portal.en.ten-opinions.16088

[22] 6 of 7 Sectoral functions were represented by national experts. Customs was represented by DG TAXUD.

[23] http://www.bluemassmed.net/

these projects are found on the indicated webpages. The purpose of these pilot projects was to test the feasibility of CISE in practice, in two sea areas, the Northern Sea basins and the Mediterranean Sea including its Atlantic approaches. Together these projects involved 14 EU Countries, Norway, and Russia as an observer, with 61 participating authorities representing all seven sectors. Both projects provided encouraging final conclusions which have been taken into account in this impact assessment.

- These pilot projects have been followed up by a new project, the on-going CISE Cooperation Project Maritime surveillance[25], involving 43 public authorities from 12 Member States and Norway. Five EU Agencies and other organisations are associated to this project. This project aims at working on issues of relevance for the establishment of CISE based on selected use cases such as information services identification, cost-benefit analysis, definition of conditions for access and specifications of common data formats and semantics. The stakeholder participation in this project continues to be high.

- Another IMP sponsored project of relevance for this policy initiative is the on-going project on the evolution of the SafeSeaNet which inter alia is assessing how this system and platform could be further developed to enhance the needs of the sectorial functions and support the National Single Window developments in a CISE concept and the further exchange of data and enhanced interoperability between relevant systems.

- The development of CISE has been discussed with stakeholders at numerous Conferences and events since 2009, including the European Maritime Day where dedicated workshops on CISE were held in 2009, 2010, 2011 and 2012. The interest and support from stakeholders in these workshops have been high.

3.3.4. *Consultancy studies*

The Commission has commissioned several specific studies on specific issues related to CISE in support of this impact assessment, inter alia a study on the IT cost of implementing CISE and a study to assess its likely impact. In addition, the Commission carried out internally a study on technical architectures and possible governance structures. These studies will become available once the policy initiative supported by this Impact Assessment becomes public[26].

The resulting assumptions underpinning the quantitative assessment of CISE are summarised in section 7.2.1 of the present report.

3.3.5 Incorporating comments from the Impact assessment board

A report was sent to the Impact assessment board on 6 November 2013.

In its opinion of 6 December 2013[27] the Board rendered a positive overall opinion but recommended that the report should be improved in order to 1) provide a clearer policy context and how this initiative relates to other relevant EU policy initiatives and identify more clearly technical and legal barriers to information exchange and the concrete consequences for the relevant sectors 2) under the baseline scenario, present more clearly the evolution of the data sharing situation across sectors and further substantiate the administrative burden

---

24   http://www.marsuno.eu/
25   http://coopp.eu/the-project
26   http://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance/index_en.htm
27   Ares (2013)3659551 of 6 December 2013

implications for national authorities, 3) explain which EU sector rules which would be targeted for legislative amendments and the views of stakeholders and 4) improve the analysis of the impacts of the policy options by clarifying the assumptions underpinning the quantitative assessment.

In a revised version of this report submitted to Inter-service consultation, these comments were addressed in the following way:

- a more detailed description of how this policy initiative relates to other relevant EU policies has been provided in the introduction.

- further details on maritime surveillance information systems have been provided in the problem definition, with examples of data currently being collected. It should be underlined however that the purpose of this policy initiative is <u>not</u> to further regulate, create new legal obligations or determine at EU level in detail which data sets that can be the subject matter of further information exchange under CISE. The purpose is simply to provide <u>the means</u> for such information exchange by ensuring the interoperability of existing information exchange systems. It is therefore for the Member States to determine which information they would like to exchange through CISE (if not already an obligation under EU rules). The reason why further cooperation is needed to develop technical interoperability solutions has been explained further.

- further concrete examples have also been added in the problem definition as well as a further clarification of the relevant legal limitations and technical barriers.

- the baseline scenario has been updated with further information on administrative burden and on service level agreements between EU agencies. However it has not been possible to make a further assessment of the evolution of the baseline scenario other than the already existing preliminary assessment by the joint research centre of the Commission since the effects can only be fully assessed once this legislation referred to has entered into force. In addition, it is not possible to make a further assessment of the evolution of data exchanges at national level since many of these data exchanges fall outside the scope of EU level intervention and since it is not intended that such data exchanges will be subject to EU level intervention other than to facilitate the means for such information exchange by ensuring the interoperability of information systems.

- the content of the policy options have been updated and are now more detailed. It has been further clarified that the intention is not to create any new data collection efforts. It is rather to reduce such efforts and data duplication by envisaging multiuse of the data being collected. Further, it has been specified that any legislative proposal to amend sector legislation or propose new legislation would be accompanied with an impact assessment. The idea of adopting a handbook as a recommendation has been abandoned for the reasons indicated by the board. However, exact indications of sectorial legislation which needed is premature and yet to be identified.

The impact of each option has been assessed further, in particular for a handbook. The administrative burden for national authorities has been reassessed. In particular, more details have been provided on how to develop IT standards for interoperability and on the involvement of Member States.

4. PROBLEM DEFINITION

4.1. The problem

The increasing challenges, threats risks and vulnerabilities[28] that the EU maritime domain is exposed to is putting additional burdens on the up to 400 relevant maritime surveillance authorities of the EU Member States to ensure the safety and security of the EU and its population. The additional workload that these authorities are confronted with is not matched with additional resources, which in turn forces them to become more resource and cost efficient.

The preparatory actions referred to in section 3 have demonstrated that the current information exchange between maritime surveillance authorities is suboptimal and can lead to efficiency losses, duplication of data collection efforts and unnecessary operational costs. In many cases, information exchange does not take place because (1) maritime surveillance authorities do not know that the information is available somewhere; (2) maritime surveillance authorities do not know that they have information of interest for others (3) it is considered too complex to do and (4), may be most fundamentally, there is no culture of doing so.

The link that would require further development, building on existing solutions and developments, relates to common standards which would allow for the interoperability[29] of sectorial systems and machine readable information services. This would further enhance the possibilities for these authorities to have access to all the information necessary for their operative work, with the indirect effect that these authorities would be able to increase their performance and efficiency in carrying out their operative tasks.[30] This goes beyond exchange of raw data (e.g. ship positions) into the further development of Information services (e.g. situational maritime picture, intelligence reports, list of suspicious vessels, risk analysis, anomalies detection, extended info on major accidents, response capacities, collaborative tools) across sectors and borders easing the tasks of national surveillance authorities in their daily duties.

The collection and exchange of maritime surveillance information (such as marine environment related information, maritime activity and event related information and security

---

[28] These can take many forms, such as natural catastrophes - storm floodings or tsunamis; security of supply related to minerals, foodstuff, seafood and energy; risks to underwater pipelines and cables through anchors, fishing gear or others; poor safety regulation of wind, wave and tidal energy farms; unintended accidents; illegal discharge of oil at sea; piracy; terrorism; local wars; illegal immigration; safety of life at sea; narcotics and arms trafficking; smuggling of (counterfeit) goods - considering that 70% of the EU's external trade is carried by sea and that stand alone cigarette smuggling constitutes a loss of public income of about €10 billion each year; importation of alien species in (polluted) ballast waters, plundering of natural resources such as overfishing; plundering of archaeological artefacts and treasures on the seabed and others. These challenges, threats, risk and vulnerabilities have been occuring on the world wide maritime areas of interest to Europe (including the Baltic, the North Celtic Sea, Biscay/Iberia, Black Sea, Mediterranean, Arctic Ocean, Oversees and High Seas) with a varying degree of frequency depending on the sea basins and the type of occurrence. More details can be extracted from expert work in the supporting consultant's study report (COWI/Wise Pen International).

[29] The term interoperability is defined in in Article 2 of Decision No 922/2009/EC of the European Parliament and of the council of 16 September 2009 on interoperability solutions for European public administrations (ISA) (OJ L260 3.10.2009) as meaning the "ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective IT systems".

[30] The consequences for the maritime surveillance authorities of this suboptimal situation is highlighted in section 4.4.

related information) by maritime surveillance authorities have historically been organised to take place <u>within</u> specific maritime surveillance sectors referred to above[31], including across borders. The information exchange within these sectors is in general terms well developed and functions well, often supported by dedicated information exchange systems at European level[32] or sometimes at regional level.

Further information on these information exchange systems are found in section 4.4. In general terms, the information exchanged through these systems can vary from one system to the next and depends on the specific control needs of each sectorial function. Such information can for example refer to ship position, composition of cargo, characteristics of vessels crew information, catch composition, storage information, disaster alert information and many more. Preparatory actions have indicated that maritime surveillance authorities across Europe are currently collecting around 500 different data sets, of which some follow from legal obligations and others are simply collected at national level to cover their specific needs.

These systems were originally constructed to enable information exchange first and foremost within single sectors, but did often not foresee information exchange with other sectors.

This picture is now gradually changing and more and more sectors are starting to share information with each other. However, as of today and as confirmed by the stakeholder consultation (see section 4.4), not all sectors involved in maritime surveillance activities have provided for the sharing of such information services to the other sectors/functions. A particular area where information exchange remains suboptimal is the exchange between civilian and military authorities. For example, Preparatory actions and interviews with stakeholders have indicated that military authorities often detect irregularities that concern civilian functions, but are often prevented from transmitting that information. This is often because the data is "over-classified" compared to how similar data is treated by civilian authorities.

In addition, the current information exchange systems do not cover all information which could be of interest to share. This means that national authorities need to find alternative ways to exchange part of the information they need to exchange in accordance with data protection requirements. Without adequate overarching IT solutions in place to interconnect the various existing sectorial interoperability solutions, like the requirement to submit defined information through the national single windows, Eurosur's National Competent Authorities, Marsur, Flux, Siena, and other systems or platforms, authorities risk to continuously be underperforming as still faced with an incoherent and incompatible patchwork of solutions, preventing automatic sharing of information services.

Member States have through surveys expressed the view that limitations to information exchange are experienced both from the perspective of the receiving and providing end user. The following figures illustrate the extent to which the different sectors are experiencing limitations in terms of exchange of information from other sectors, within Member States. The black line in the depicted bars is calculated as each sector's average limitation value in terms of access from all other sectors, across all Member States. The position of the bar indicates the minimum and the maximum data limitation that the sector experiences from another sector (in averages across Member States).

---

[31]   See introduction, in other words general law enforcement, border control, maritime safety/maritime security and prevention of pollution caused by ships, marine pollution preparedness and response/marine environment protection, fisheries control, customs and defence.

[32]   See section 4.4.

Average limitations felt towards each sector in terms of providing data access (within Member States)

Experienced limitations of user communities in terms of access to information from the other user communities (within Member States)
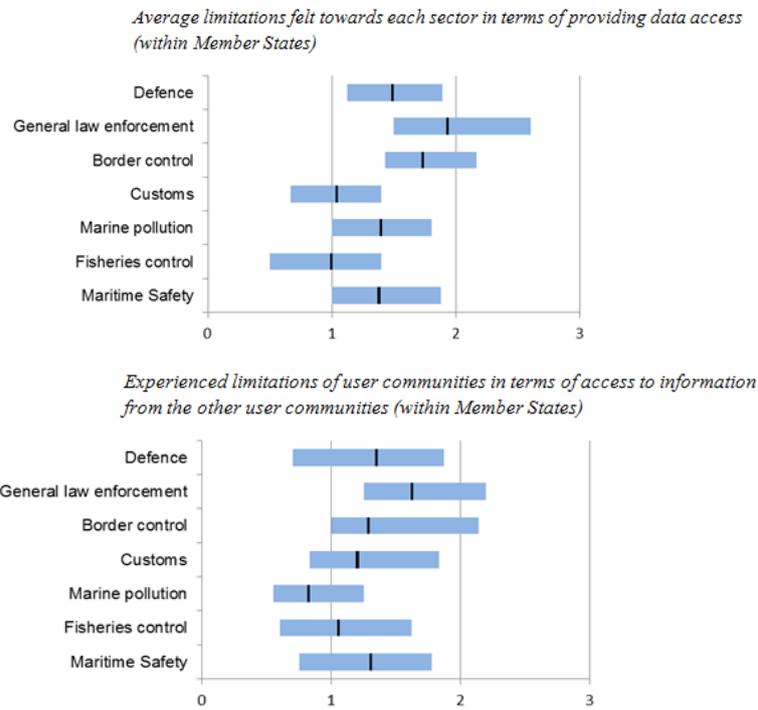
*Note: 0: never; 1: rarely; 2: occasionally; 3: often*

Figure 1- Limitations in access to information (source: Member States survey)

The experienced limitations are generally larger when looking at data exchange between Member States.

The problem statement can be illustrated by the following practical examples from the preparatory actions and stakeholder consultations:

Maritime surveillance authorities claim that they have suboptimal access to the maritime surveillance information needed e.g. for the optimum planning of their routine operations and for their various interventions at sea. Some of the information relevant for this planning is not easily accessible or not accessible at all due to real or perceived legal limitations or technical or cultural barriers, depending on each Member State. Information needed for these tasks are typically: (1) Internal surveillance capacities (patrol vessels, aircrafts, including relevant capacities of other partner authorities within a given sea area), (2) historical information about maritime activities in that particular period of the year (organized by own entity or other entity), (3) respective planning of partner authorities (e.g. navy, police), if available, (4) programmed services offered by EU agencies (e.g. satellite images), stand-by antipollution vessels or possible deployment of means at sea (either directly or e.g. through the national maritime surveillance centres) (6) info about tides and extreme weather forecasts, (7) navigational warnings, military exercises, other restricted areas, (8) possible risk assessments carried out by other national authorities or EU agencies, (9) list of suspicious vessels.

In addition, coordinated information services from neighbouring countries may be needed, in order to avoid overlapping activities. Co-ordinated patrol activities near the border and coordinated risk assessments which might affect the own area of responsibility are of particular interest as well routine access to coastal radar or visual imagery from those countries, and planned satellite image service.

Another example is a pleasure boat approaching the European continent from the Atlantic Ocean can potentially be smuggling drugs or arms or be in violation of any other rules of the

19

seven maritime surveillance sectors. It may enter the EU at any place along its coastline from the Gulf of Finland to the Black Sea. Customs and other maritime control authorities along these coasts may be in a difficult position to detect violations unless receiving appropriate information from partner authorities in other sectors as to the suspicion of any nature of the violation, the name of the ship, its destination and its time of arrival.

4.2. What is causing this problem?

The problem is driven by a number of specific causes. The most important specific causes are the following:

Cause 1: Real or perceived legal limitations and legal uncertainty to information exchange between the relevant maritime surveillance sectors

As mentioned above, the different sector policies dealing with maritime surveillance have been developed relatively independently from each other in accordance with the division of competence between authorities at national and EU level. The result has been a lack of synergies between sectors/functions in general and in particular, this approach has not allowed for or created channels for information exchange between them. Instead, sector legislation at national and EU level has often been drafted in such a way that information exchange with other sectors either is not promoted or in some cases not even allowed.

Although the picture is now gradually changing and more and more sectors are starting to share their information collected with other sectors, the current EU regulatory framework has still very variant approaches to information sharing from being direct obligations to share certain data with other sectors to directed prohibitions to do so. There are mainly four categories of real or perceived limitations to information sharing between sectors: 1) direct legal limitations for sharing of information with other sectors 2) provisions exempting specific functions of data sets from any sharing arrangement, 3) legislative acts being silent on the issue (interpreted as meaning that sharing with other sectors is not possible), and 4) provisions which open for sharing with other sectors but not in a mandatory form.

These categories can be illustrated by the following example:

An article 12 was introduced in the fisheries control Regulation of 2009[33], stipulating that certain defined control data (VMS, AIS and VDS data[34]) collected within the field of fisheries "may be transmitted to Community agencies and competent authorities of the Member States engaged in surveillance operations for the purpose of maritime safety and security, border control, protection of the marine environment and general law enforcement".

On the one hand, this Article ensures the sharing of the identified data to other functions and provides for a legal basis of such sharing (to address categories 1 and 3), but on the other hand limits the sharing to certain data and only on a voluntary basis (which might not address categories 2 and 4).

It can be noted at the same time that the conditions for exchanging data with other sectors depend on the nature of the data. Non sensitive data can always be shared more easily with other sectors than sensitive data (most often personal data or commercial data), for which the conditions for access always have to be coupled with the need to know principle referred to above. If the sharing of information involves the processing of personal data, the EU law on

---

[33]   Council Regulation (EC) No 1224/2009 of 20 November 2009 establishing a Community control system for ensuring compliance with the rules of the common fisheries policy
[34]   Vessel Monitoring System, Automatic Identification System and Vessel Detection System data

protection of personal data[35] and the national legislation implementing this EU law are applicable. This means in practice that perceived legal limitations (such as the limitation in the above Article 12 to limit the distribution of data to certain data sets) in fact are justified. Moreover it has to be noted that the exchange of personal data has to comply with fundamental rights, including the protection of personal data. This is of essential importance with regard to the necessity of data processing in the light of data protection principles such as the 'purpose limitation' for processing operations.

Another challenge is to determine if the limitation is found at EU level or national level. A limitation which is perceived as an EU level issue can in fact primarily be a national matter. This can be illustrated by the following example from preparatory actions:

A national surveillance aircraft operating under the border control scheme of Frontex detects and illegal transhipment activity between a fishing vessel and a cargo vessel. In some cases, the national inspector operating under the Frontex regime has considered that he/she is neither allowed to intervene nor report this incident to fisheries authorities. If the fisheries authorities nevertheless are alerted by phone, fisheries authorities will have to send out a separate plane to record the incident and conduct an inspection, to an extra flight cost of several thousands of euros per hour.

This problem can be perceived as an EU level problem since the inspector is operating under the Frontex regime, but is in fact likely to be a national problem since there are no Frontex rules which prevent the national inspectors from intervening on other matters than border control. The limitation lies instead with how the mandate of the inspector has been formulated at national level. In such a case, the limitation is more of a cultural limitation and not an issue that can be dealt with through legal action at EU level.

A screening of EU legislation made under this impact assessment has shown that most or all direct legal limitations to information exchange have already been removed or are in the process of being removed and that a necessary legal basis for information exchange is being put in place (such as Article 12 of the Fisheries control Regulation). Legal limitations therefore mainly refer to national legislation as shown in the above Frontex example.

Cause 2: absence of an appropriate IT environment which ensures the interconnectivity of existing and future systems.

The seven sectoral functions carrying out maritime surveillance activities are making extensive use of IT solutions to support their activities. 72 systems have been identified through the Member States survey referred to in section 3. These IT solutions have however been developed independently from each other, with a data collection programme tailored only for each sectorial function. In other words, these information systems lack interoperability and the missing link is a common communication tool and a data model. If one compares with the Internet, this tool is the Http protocol. The lack of homogeneity between the IT systems means that information exchange between them becomes compromised, with the effect that maritime surveillance activities become less efficient. This was confirmed by both the Member States survey and the public consultation.

---

[35]   Article 8 of the Charter of Fundamental Rights of the European Union; Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data: the national legislations which implemented Directive 95/46/EC; Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters; Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

In fact, the lack of a European wide infrastructure interconnecting maritime surveillance authorities based on common standards led to the creation of specific and different solutions ensuring the information exchange within each sectorial function. This means that within most sectoral functions, EU-wide systems are already in place, and are supporting day-to-day activities, as a complement to national IT solutions.

For example, the Maritime Safety and Security community facilitates cross-border exchange between Member States with the "SafeSeaNet"[36] solution and the "National Single Window"[37] (the maritime "National Single Window" is currently defining an information exchange platform to facilitate port reporting formalities for ships and information exchange between relevant authorities belonging to maritime safety and security, customs, border control and health communities within a Member State and between Member states); also a study as regards the "SafeSeaNet evolution" including a "National Single Window demonstrator" is ongoing by EMSA but preliminary and meant to be submitted to TAG once sufficiently advanced; the Border Control community with the" European border surveillance system" (EUROSUR)[38]; the Customs community with the "Common Communication Network and Common System Interface" (CCN/CSI)[39]; the Defence community with the "Maritime Surveillance" network (MARSUR); the Marine Environment community with the "Infrastructure for Spatial Information in the European Community" (INSPIRE)[40] and the "Shared Environmental Information System" (SEIS)[41]; the Law Enforcement community with the "Secure Information Exchange Network Application" (SIENA); the Fisheries Control community with the "Data Exchange Highway" and its "Fisheries Language for Universal eXchange" (FLUX). Beside this variety of IT solutions at national, regional or European level, the total number of stakeholders (more than 400 public authorities across the EU/EEA, IT providers, shipping industry…) makes the situation even more complex when it comes down to exchanging information between their IT solutions. All the systems at national level (72 reported from the survey – see above) have been designed without ensuring their interoperability, i.e. there are 72 different ways of describing and modelling similar information. At EU level, the interconnection solutions described above have also to a great extent been put in place without ensuring their interoperability. This means that different way of describing and modelling similar information has been created in each system (e.g. a vessel is described differently in each of these EU interconnection solutions).

Until now, interconnecting these IT solutions –whenever envisaged- has mainly been done by establishing specific interfaces. But such way of "stitching it together" does not work if cooperation is envisaged at a larger scale cross sector. It is to be noted that the Port Reporting

---

[36]　Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC.

[37]　Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC. The national single windows will be fully functional in Member States by 1 June 2015.

[38]　Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR).
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011PC0873:EN:NOT

[39]　Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes.

[40]　Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)

[41]　Communication from the Commission to the Council, the European Parliament, the European economic and social Committee the Committee of the regions: Towards a Shared Environmental Information System (SEIS) COM(2008) 46 final – 01.02.2008.

Formalities Directive introduces a better interoperability approach and requires the development of "National Single Window" in each Member State compliant with common specifications for information exchange. However the "National Single Windows" do not cover all the functions relevant for maritime surveillance. They will provide Member States with maritime transport related information. They will not allow for information exchange between for example a border control authority in one Member State and a navy or fisheries authority in another Member State. The problem at hand is the "**lack of semantic and technical interoperability between IT solutions used to support maritime surveillance activities**"*:*

- Semantic interoperability is jeopardised by different interpretations of the information exchanged between administrations, people, and applications. The lack of a consistent format for the electronic exchanges increases the complexity of the interconnection of the IT solutions (or analysis by humans).

- Technical interoperability is jeopardised by the variety of IT solutions and technologies and the absence of agreement on how to automate information exchanges in a uniform and consistent way.

Such lack of interoperability is the result to sub-optimal cross-sector cooperation. Further cooperation on the definition of common standards to improve interoperability is therefore necessary.

A practical real example of what the consequences of this lack of interoperability could be is the following: A maritime surveillance authority in Member State A would like to share information with an authority in Member State B. It generates a document (e.g. a Word document) then sends the document as an attachment to an email. The receiver then prints the document and re-encodes it manually into its own maritime surveillance system. The result is that the message is not being timely processed, that there could be encoding errors and that this work would take time at the expense of the execution of the core maritime surveillance activities. In a digital world, all these steps can occur electronically and automatically.[42]

The European Commission is currently implementing an overall strategy to rationalise and streamline the IT systems it develops, maintains and operates, including systems supporting EU policies and the information exchanges between European Public Administrations (at European and national level)[43]. The rationalisation initiative of the "trans-European systems between administrations" might lead to the convergence of existing solutions (or some of them) to a common architecture, to a common infrastructure and to building blocks offered to interconnect public authorities. Given the fact that the convergence of the solutions in place will take a long time, it is imperative that the problem of interoperability in maritime surveillance gets addressed today.

Cause 3: Cultural and administrative barriers
This cause refers to the organisational structures of administrations and the behaviours and mentality of individual officials. Discussions so far around the CISE project have shown[44] that there has been a tradition to keep surveillance information within functions and that the willingness to exchange information ("dare to share principle") between functions has been

---

[42] Some encouraging developments can however be noted which permits automatic transmission of information, inter alia through the use of National Single Windows, Eurosur, Marsur, Flux, Siena, as well as other systems and platforms referred to in this text.

[43] Assessment of Trans-European networks supporting EU policies, under the Interoperability Solutions for European Public Administrations programme (ISA): http://ec.europa.eu/isa/actions/02-interoperability-architecture/2-14action_en.htm

[44] See in particular MARSUNO pilot project final report - http://www.marsuno.eu/

relatively limited. There are substantial variances between Member States on the willingness to share information, although more difficulties seem to occur in Member States with high hierarchical organisational structures.

This lack of willingness to exchange information with other functions is often the result of a lack of trust and confidence and a lack of common cultural knowledge and understanding of the operational aspects of other sectors. Another explanation often referred to is that inspectors in some countries do not feel that they can share the information in the absence of an explicit legal basis. Other factors include different interpretations of terms and concepts used as well ignorance of organisational structures, working methods and political cultures of the partners. The fact that maritime surveillance activities have been organised sector by sector in a rather isolated way has contributed to this cultural distrust.

4.3. Who is affected by the problems and what are the consequences for them?

The number of authorities dealing with maritime surveillance information in any form has been estimated to be around 400 (see list of authorities in Annex 3). These are essentially EU and EEA Member State authorities, but include also a number of EU Agencies (concerning the relevant EU agencies, see further section 4.5.2 below). This does not include research bodies which might need maritime surveillance data for scientific purposes, such as fish stock assessments or assessments of the state of the marine environment.

Further, all economic actors and citizens in the EU/EEA are indirectly affected by this suboptimal situation as any threat to EU/EEA either at sea (in Member States' waters or in any international waters of EU interest) or entering EU/EEA territory by sea may affect these actors' security, economic, social and environmental interests.

The direct result of this suboptimal situation for these authorities is that they often have an incomplete overview of the maritime awareness situation in the area in or for the activities for which they are responsible.

Incomplete maritime domain awareness can have, inter alia, the direct following operational consequences:

1.   Authorities remain unaware or incompletely aware of threats under their responsibility despite that information that would be relevant for their operative activities is available in other sectors. Their maritime domain awareness is sub-optimal.

2.   Threats may not be detected, checked and thwarted in time despite that relevant information is available in other sectors.

3.   Limited response capabilities and cost-savings in the use of assets leading to parallel, uncoordinated and less efficient deployment activities which can have negative spill over effects for the surveillance of other sea areas or other duties (e.g.: an hour flight of a surveillance aircraft costs several thousands of euros).

Concretely, the negative consequences for these authorities are less efficient surveillance outcomes i.e. less success rate in detecting, checking and thwarting on risks/events such as: death toll at sea; illegal immigration; arms and drugs smuggling; illegal, unreported and unregulated fisheries; sea borne pollution; piracy attacks, etc. In other words, it means that surveillance activities risk being response oriented instead of being anticipative or predictive. A concrete example where surveillance activities need to become more anticipative is the influx of irregular immigrants through the Mediterranean. Early information e.g. from navies or any other sector of the whereabouts of vessels carrying irregular immigrants could for

example have helped preventing tragic events like the tragic events near the island of Lampedusa in late 2013 when many hundred irregular immigrants lost their lives.

In addition, suboptimal exchange of surveillance information between the relevant authorities can have the following administrative consequences:

1.   Duplication of work and costs: several authorities collect the same data as other services in support of their activities.

2.   Excessive administrative cost (e.g. manual encoding in systems) and reduced cost efficiency leading to resource shortages on other tasks. This includes cost of operating several different IT solutions for the different sectorial functions for the same purpose of information sharing.

4.4.   The baseline scenario

The Technical Advisory Group referred to in section 3 has in 2011 elaborated a gap analysis covering about <u>five hundred generic data elements</u> relevant to maritime surveillance[45].

The purpose of this very extensive exercise was to make an inventory of the different data sets which is being collected by the different sectorial functions at national level in order to 1) identify duplication in data collection efforts, 2) to verify which information is already being exchanged with other sectorial functions and 3) if there was a demand[46] from the other 6 sectorial functions to receive such information which was not yet exchanged. The inventory contained a list of the most relevant generic maritime surveillance data sets which could be relevant for information exchange across sectors and borders in the EU/EEA.

The result of this gap analysis was that there is a potential gap of between 40% and 90% between supply and demand for additional data exchange between the sectorial functions depending on the area and that 45% of currently collected information is collected by more than one sectorial function, and that about 80% of the existing information is in national ownership. Moreover, almost half of the information that is gathered is owned by two sectoral functions, namely defence and maritime safety, security and prevention of pollution by ships.

The frequency of these information supplies/demands varies as some information might not be needed on a regular basis.

---

[45]   It is available at https://webgate.ec.europa.eu/maritimeforum.

[46]   When requested to identify the relevant demand, TAG participants were requested to limit themselves to information for which it could be considered that the sharing of information could correspond to a justified operational need in accordance with the need to know principle referred to above. It is to be noted that this assessment is indicative only since the expected demand might not fully correspond to the actual right of the owner to share this information due to confidentiality requirements. It was not considered possible to make a full assessment if the owner of the information had to share the relevant information since that assessment has to be made by him of the data on the basis of a case by case analysis of the relevant data. Therefore, it will ultimately be for the demand side and for the owner to determine which information can be shared by the owner and whether the receiver has a justified need to receive it.
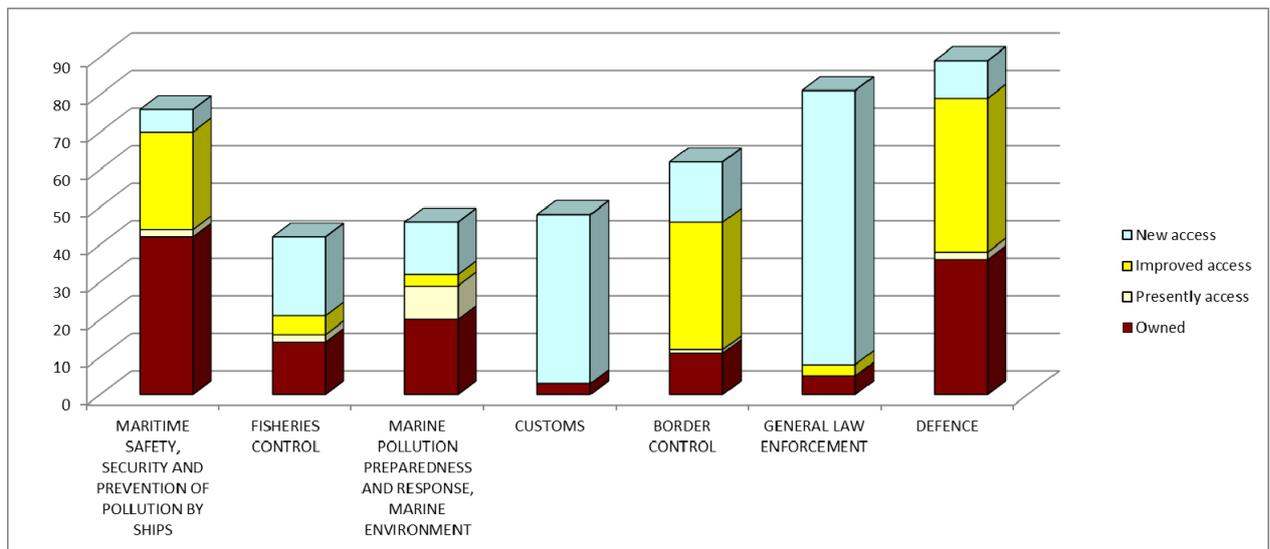
Bottom (dark red): data presently owned by the sectoral function.

Lower centre (light yellow): data presently received from other sectoral functions.

Upper centre (yellow): data presented partially received from other sectoral functions; but there is still a need to improve the completeness of the collection of this data.

Top (blue): data not exchanged at present but requested from other sectoral functions.

Figure 2 - Overview of data gap assessment (source: TAG work)

As explained above, there have been some further developments since this gap analysis was made in 2011. In particular, one can note the adoption of the ship reporting formalities Directive (referred to above) for maritime transport - which will put in place "National Single Windows" in Member States by 1 June 2015 - is expected to reduce the gap identified for this sector as well for the maritime safety and security, customs, border control and health sectors to some extent by introducing the sharing of all ship related regulatory information for vessels above 300 gross tonnes between national authorities and exchange between Member States. A very preliminary assessment made by the Joint Research Centre of the European Commission has concluded that this new system will reduce the said gap from a range of 40%-90% range to a range of 30%-85%[47]. Further, as regards the particular gap related to customs, the result remains uncertain since the assessment of the data supply and the data demand was not complete and made with different premises.[48]

There are also other sectoral EU-wide systems and platforms for information sharing that have been put in place, and many are highly functional and successful. Some have started to look at the opportunity for including other sectoral functions but there is no EU wide approach to this.

---

[47] This estimation is made with the assumption that the single window will in the future be able to share information with all the 6 other functions. The current directive provides for sharing with the customs and border control communities only.

[48] Whereas the supply side has been defined as the data required by the Community Customs Code and its implementing provisions for the declaration of goods, the demand side has been identified from the perspective of what could be needed from a more operational point of view by national customs authorities engaged in preventive activitites in case of an event, in addition to those already accessible in accordance to EU law.

4.4.1.   Evolution of the baseline scenario

Efforts to ensure enhanced cross sector information exchange between maritime surveillance authorities has already been going on for some time, but has accelerated with the development of the Integrated Maritime Policy of the EU, where exchange of maritime surveillance information was considered a priority issue.

In fact, the efforts to bring together technical maritime surveillance experts from different sector policies, inter alia through the creation of a Member State Expert sub-Group and a Technical Advisory Group[49], pilot projects and the publication of two Communications from the Commission[50], have increased interest in information exchange between sectors and helped increase confidence building to work closer together.

Consultations with Member States through focus groups have shown that individual Member States have started to move away from the traditional silo thinking when treating maritime surveillance information at national level. Many Member States are instead taking steps to enhance information exchange between sectors, and some have already put in place, or are planning to do so, national coordination centres and common information sharing environments (e.g. Finland, United Kingdom and Portugal). The willingness to share information across sectors has been increased, but some hurdles are still encountered. These particularly concern unrecognised information needs of other sectoral functions; lack of common definitions and standards as well as lack of trust between the sectoral functions.

At EU level, pilot projects and requests from different entities such as EUNAVFOR, FRONTEX, EFCA, EUROPOL or Bonn Agreement on pollution control in the North Sea[51] as well development of other EU initiatives[52] has contributed to increased co-operation.

Furthermore, two directives the Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and the Directive 2010/65/EU on Reporting formalities for ships arriving in and/or departing from ports of the Member States, are particularly significant in the context of maritime awareness as those facilitate the collection, sharing and exchange of information on all ships above 300 gross tons[53] (except military) on their identification, movement, status (crew and passenger health, ship safety, ship security and environment related),cargo, crew and passengers between authorities. Directive 2002/59/EC is currently under review in order to assess the Union maritime information and exchange system "SafeSeaNet" and how it can be enhanced and further used for the intended purposes of safety, security, pollution prevention and maritime transport as well as maritime traffic and trade, already involving various sectorial functions depending on the national organisational structure. At the same time, EMSA is developing the "Integrated Maritime Data Environment"[54] as a technical framework that collects and combines data from EMSA's maritime applications to provide

---

49	Referred to in section 3 of this report.
50	See footnotes
51	See further http://www.bonnagreement.org/
52	Such as project MARSURV-1: anti-piracy monitoring service off the coast of Somalia for Atalanta operation with EUNAVFOR (EU Naval Forces); project MARSURV-2: EU maritime borders surveillance service in the Mediterranean for INDALO operation with FRONTEX and project MARSURV-3: fisheries control service with EFCA in the Mediterranean during the bluefin tuna surveillance campaign; project BE-AWARE: risk assessment of marine pollution in the North Sea and its approaches .
53	While such big ships have a primary economic importance, it has to be noted that the majority of ships subject to maritime surveillance are smaller than 300 gross tons. These include small fishing vessel, pleasure craft and too often small boats carrying illegal immigrants over sea.
54	http://www.emsa.europa.eu/integrated-maritime-data-environment-imdate.html

integrated maritime services and a more complete maritime awareness picture, tailormade in accordance with the demands of various sectoral functions.

As required by Directive 2010/65/EC, the Member States are currently implementing "National Single Windows" for ship reporting formalities. Information will be reported electronically and only once by the ships. These "National Single Windows" will be linking "SafeSeaNet", e-Customs and other electronic systems. Vessel related information will be made available to relevant authorities (maritime security and safety, customs, border control, and health) within a Member State and between Member States. These "National Single Windows" will be fully operational from 1 June 2015.

Accordingly, Service Level Agreements have been established between EMSA and FRONTEX, EMSA and EFCA, and EFCA and FRONTEX to support them respectively in enhancing their knowledge of the maritime domain awareness. These agreements cover a number of areas for mutual cooperation, such as the integration of various control data such as satellite AIS, radar images position reports from the VMS and AIS systems. These data are combined through joint nautical charts[55].

However, although improving the situation, it is not expected that these developments, in the absence of an interoperability framework between existing systems with common standards for machine readable exchange of information services, will be capable to fully meet new challenges and address the problems identified in this section effectively. The result would be that increased threats and risks would not be dealt with in the most effective manner, that potential conflicts between central EU policy objectives would persist and that duplication of data collection efforts will continue to exist. These developments, already required by EU law in some cases, do however constitute important building blocks and will be the point of departure for the construction of such an interoperability framework.

As regards the evolution of IT technologies, there are two main drivers for the evolution of IT systems[56]: supply-side drivers (technology development or technology retirement) and demand-side drivers (new business functionalities). Given the projections of increased risks and threats in the coming years[57], this suggests that there is a growing need for new business functionalities and therefore a need to invest in IT systems to support better operations. The initial investment cost in an IT system on average is 8% of the lifecycle cost of that IT system and that the lifecycle of an IT system is typically 15 years[58]. The Member States survey shows that the average age of national IT systems supporting maritime surveillance activities is 8.7 years, which also suggests that several IT systems will have to be replaced in the future.

However, the evolution of IT systems is impossible to foresee and the baseline assessment shall only take into consideration current, planned or highly expected evolution scenarios. One needs also to take into account that in a situation of financial crisis, several Member States might not be in a position to make the necessary investments to meet these new IT demands. If the IT requirements cannot be met, the effectiveness and cost efficiency potential offered by CISE cannot be reaped.

In addition, the IT technologies and standards used in the Member States risk evolving in an incoherent way. This suggests that the administrative burden of putting in place additional

---

[55]   Further information on the content of these agreement can be found in the study in support of this Impact assessment.

[56]   "The Four Laws of Application Total Cost of Ownership", Gartner, Andy Kyte, 3 April 2012 (reference ID G00230382)

[57]   See risk assessment study referred to in footnote 26.

[58]   See Gartner study on the "Sustainability and Efficiency of Visions for CISE" for more information, available on http://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance/index_en.htm

information exchanges and building new IT functionalities will be high and not cost-efficient. This has already happened in the recent past with several interconnection solutions put in place by the EU (EUROSUR, National Single Window), where the interoperability concerns have not been addressed in a sufficient manner. The administrative burden imposed to the Member States can be considered as unnecessarily high, since different IT solutions are developed by different sectors.

4.5. EU right to act, added value, proportionality and subsidiarity

4.5.1. The right to act – treaty basis

If the preferred option of this impact assessment will be to exclude any legislative action as defined in Article 288 of the TFEU and instead adopt a consultative initiative such as a Commission Communication, it is not necessary to define any legal basis for such a policy option.

If however legislative action is considered as a preferred option in this impact assessment, it will not be feasible to incorporate relevant legal provisions of the CISE project into single instrument given that there is no basis in the TFEU for all seven sectoral functions. The defence policy falls outside the TFEU and falls only partially under the TEU while most of it falls under direct national competence. Moreover, some Member States have an opt-out clause for anything that falls under border control and justice co-operation[59].

In addition, measures can only be included in the same instrument when the relevant process for adoption of the legislative instruments at issue is the same, they have the basis in the same Treaty and are of the same nature.

Therefore, the most feasible approach for legislative action seems to be to elaborate a legislative package containing instruments based on the respective Articles of the Treaty the subject matter fall under and in accordance with the procedures and under the conditions envisaged.

It is worth noting also that the CISE project is developed under the Integrated Maritime Policy of the EU. Legislative initiatives so far developed under this policy have been proposed with a multiple legal basis, representing those sector policies which affect our coasts, seas and oceans. It is settled case law that when a measure simultaneously pursues a number of objectives or has several components that are indissolubly linked, without one being secondary or indirect in relation to the other, such an act will have to be founded on the various legal basis.

A multiple legal basis instrument can in this specific case come into play when measures referring to 2 or several sectors "fall in the same basket" i.e. refer to the same Treaty, are of the same nature (Regulation or Directive) and follow the same legislative procedure for adoption.

4.5.2. Added value of EU action

The added value of EU action has been widely recognised already in stakeholder consultations in other various events and consultations referred to in Section 3.

Information exchange between maritime surveillance authorities are to a large extent of a transnational nature since it normally entails co-operation first and foremost at regional or sea basin level.

---

[59]   Denmark, the United Kingdom and the Republic of Ireland.

Moreover, rules and conditions for transnational sharing maritime surveillance information mainly between authorities of a same sector are already regulated at EU level; which means that amendments of the regulatory framework and the possible removal of legal limitations in accordance with data protection requirements will have to take place at the same level.

In addition, a number of EU Agencies are involved in maritime surveillance activities and are therefore a part of the already existing information exchange at sector level. Several EU agencies and similar bodies are directly relevant for the CISE project, such as EMSA, EFCA, FRONTEX, EDA and EEA.

The process therefore requires an overall EU and EEA wide direction, an overall management of diversity in order to ensure that information exchanges are efficient and beneficial for all maritime surveillance authorities across Europe, independently where threats might occur.

Without targeted action at EU-level it is not likely that transnational issues can be resolved and co-operation ensured in an efficient manner.

4.5.3. *Subsidiarity and Proportionality*

The principle of subsidiarity is very relevant in this case. Prior consultations with Member States have concluded that, although targeted EU action is necessary to ensure the interoperability of the current system, the operational aspects of any future common information sharing environment needs to be decentralised. This is due to the fact that the operational information exchange most often takes place between national authorities, although some interaction also occurs with EU agencies when they handle maritime surveillance information based on EU sectorial Regulations.

The role of the EU should therefore essentially be to act as a facilitator, to ensure coherence and common standards and to review and revise relevant EU level legislation when necessary.

In conclusion, it is not intended that the CISE project will interfere with the organisational or operational aspects of maritime surveillance related information exchange activities at national level to a larger extent than today. The focus of this work on this policy initiative will be on the EU level. Member State authorities can however make use, as they see fit, of the solutions that can be achieved at EU level.

As regards proportionality, EU action to develop a common information sharing environment will not go beyond what is necessary to achieve the objectives. Measures need to be developed with the right level of detail without micromanaging the process.

Measures should not go into more detail than what is the case for the current information sharing mechanisms within sectors.

4.5.4. *Coherence with existing policies and initiatives*

The CISE project is intended to be built on current achievements and the existing mechanisms for information sharing which have already been developed at sector level. The purpose will be to ensure the interoperability of sector systems without reinventing any wheels but to streamline over time and reduce administrative burden. This is to realise the full potential of existing resources primarily in terms of sectorial policy achievements, but also better cross sectorial knowledge of occurrences in particular sea basins and to create new business opportunities.

Furthermore, the project is fully in line with a number of other EU wide initiatives such as, the Blue Growth initiative[60], the Marine Strategy Framework Directive[61], the proposal for a

---

[60]   See for example the Ministerial Limassol Declaration referred in footnote n°17 and Communication from the Commission to the Council, the European Parliament, the European economic and social

Directive on maritime spatial planning and integrated coastal management[62], the EU Maritime Transport Strategy 2018[63] including the Community vessel traffic monitoring and information system Directive[64] and the reporting formalities for ships arriving in and/or departing from ports of the Member States Directive[65] as well as the EUROSUR Regulation[66] and customs legislation[67].

The CISE project also operates within a larger framework of EU-level policies and strategies on eGovernment that have been developed in recent years (see Annex 4):

- The Malmö and Granada Declarations[68] on eGovernment, encouraging the development of more efficient interoperable public services and the European eGovernment Action plan 2011-2015[69].
- The Digital Agenda for Europe (one of the flagship initiatives of the Europe 2020 Strategy) where seamless cross-domain and cross-border information exchanges are a priority for the EU. The CISE initiative facilitates Pillar I - *Digital Single Market*, Pillar II - *improving standard-setting procedures and increased interoperability* and Pillar VII - *IT-enabled benefits for EU society*.
- The strategy of the European Commission to rationalise and streamline the IT systems it develops, maintains and operates.
- The ISA Programme[70] aiming at fostering interoperability between public administrations. The CISE project has been funded as relevant action in the Trusted Information Exchange area.

In addition it is part of the recent Action Plan to increase the competitiveness of the EU Security and Defence sector[71+68]. It will be also part of cross-sectorial cooperation areas to implement the future European Union Maritime Security Strategy[72].

Committee and the Committee of the regions: "Blue Growth: opportunities for marine and maritime sustainable growth" COM(2013) 510 final – 08.07.2013

[61] Directive 2008/56/EC of the European Parliament and of the Council of 17 June 2008 establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive)

[62] Proposal for a Directive of the European Parliament and of the Council establishing a framework for maritime spatial planning and integrated coastal management COM(2013) 133 final – 12.03.2013

[63] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Strategic goals and recommendations for the EU's maritime transport policy until 2018 - /* COM/2009/0008 final */ 21.01.2009

[64] See footnote n°36

[65] See footnote n°37

[66] See footnote n°38

[67] See Community Customs Code (OJ L 302, 19.101992, p. 1). This Customs Code will soon be superseded by the recently adopted Union Customs Code (OJ L 269, 10.10.2013, p.1) which will come into force on 1 June 2013.

[68] Malmö Declaration: http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf
Granada Declaration: http://ec.europa.eu/ceskarepublika/pdf/press/ks7rada.pdf

[69] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:PDF

[70] Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on establishing a programme on interoperability solutions for European public administrations (ISA) — OJ L 260, 03.10.2009, p. 11.

[71] Communication from the Commission to the Council, the European Parliament, the European economic and social Committee and the Committee of the regions: "Towards a more competitive and efficient defence and security sector" /* COM/2013/0542 final */ 24.07.2013

Last but not least, the CISE initiative is in line with the European Interoperability Framework (EIF)[73], which is promoting and supporting the delivery of European public services by fostering cross-border and cross-sectorial interoperability. It defines four levels of interoperability, which deserve special attention when a new European public service is established. These levels are described as follows:
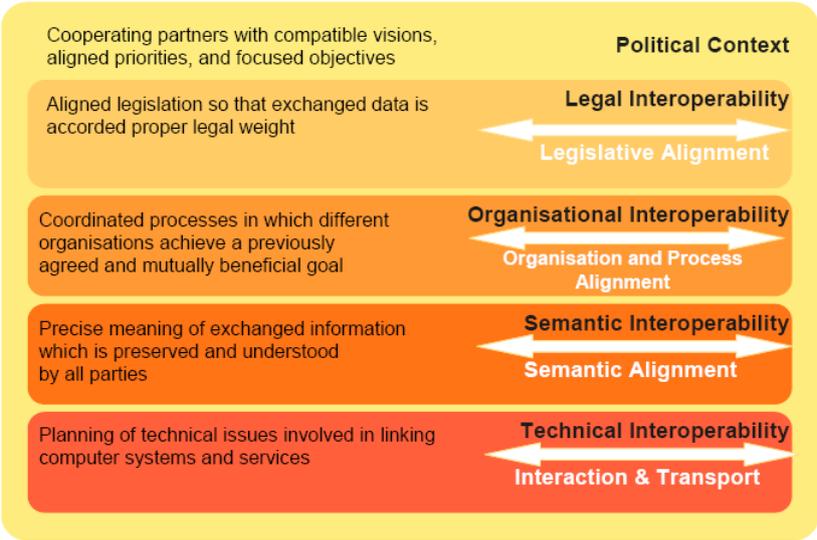

Figure 3 - European Interoperability Framework (source: Commission)

5. OBJECTIVES

5.1. General objectives

The general objective of this policy initiative is to ensure that maritime surveillance information and services collected by one maritime sector and considered necessary useful for the activities of other maritime sectors can be efficiently shared with those sectors.

The point of departure should be the current achievements and already existing standards for information exchange and work should focus on ensuring the interoperability of information exchanges regulated at EU level, with a particular view to provide Member States with interoperability solutions that they may apply at national level. A particular objective would be to enhance information exchange between civilian and military authorities.

Enhanced information exchange between sectors is expected to contribute to a better overview of the maritime domain awareness for the maritime surveillance authorities at national and EU level and enhanced consistency between sector policies in line with the Integrated Maritime Policy of the EU and facilitate "smarter surveillance" by more anticipative and predictive activities.

The foreseen exchange of information between sectors will have to respect the same rules and principles as for data exchanges within sectors, in particular the relevant provisions of the EU

---

[72]   Joint Communication from the Commission and the High Representative of the Union for the Foreign Affairs and Security Policy to the European Parliament and Council: Elements for a European Union Maritime Security Strategy: For an open, safe and secure global maritime domain – planned to be adopted early 2014.

[73]   The European Interoperability Framework 2.0 (http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf), as an annex to the Commission Communication on Interoperability for European public services, defines semantic interoperability as the precise meaning of exchanged information which is preserved and understood by all parties and technical interoperability as the planning of technical issues involved in linking computer systems and services.

Charter of Fundamental Rights[74], the EU legal framework on the protection of personal data, and the national legislation implementing this EU law, as well as the relevant provisions for the protection of commercially sensitive data.

Personal data can only be exchanged if the processing is legitimate[75] and if certain principles relating to data quality are respected[76]. As the purpose of CISE would be to enhance the sharing of information between maritime authorities, it is of particular importance to ensure that strict safeguards are in place whenever personal data are transferred. Therefore, information which contains personal data may only be exchanged for very specific purposes. Also the principle of data minimisation[77] has to be respected, which means that only that personal data will be exchanged which will really need to be exchanged to achieve the defined objectives.

Commercially sensitive data can only be exchanged if the processing does not undermine the economic interest or competition position of the owner of the information.[78]

No free flow of information between sectors is thus envisaged.

Within the field of fisheries, personal data could for example be data on fishing vessels which directly or indirectly identifies the characteristics about the crew. Commercially sensitive data could for example be the exact position reports of fishing vessels which identifies attractive fishing grounds.

Indirectly, a Common Information Sharing Environment is very likely to trigger enhanced cooperation[79] between maritime surveillance authorities leading to increased operational efficiency and cost effectiveness, for example by eliminating duplications of data collection efforts or by coordinating deployments of assets such as ships, aircrafts and satellites in a given sea area.

Since the objective of this initiative is limited to ensure the interoperability of existing and future maritime surveillance systems, the intention is not to develop any new maritime surveillance system. Nor is it intending to replace existing or planned systems and or to duplicate existing or planned systems. It is not intending either to gather more information through own sensors nor permanently store maritime information. It is not intending either to

---

74   http://ec.europa.eu/justice/fundamental-rights/charter/

75   Article 7 of Directive 95/46/EC. This means that processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority

76   Article 6 of Directive 95/46/EC. This means that data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; the personal data must be adequate in relation to the purposes for which they are collected and kept no longer than is necessary for those purposes

77   Which follows from Article 6 of the Directive 95/46/EC.

78   Commercially sensitive data is commonly referred to as any information which is not in the public domain or publically available and where disclosed may undermine the economic interest or competition position of the owner of the information. See for example the guidance document by the European Medicines Agency on the identification of confidential information and protection of personal data www.ema.europa.eu.

79   As elaborated in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "Towards interoperability for European public services" (COM(2010) 744 final) – 16.12.2010:
"For public administrations, interoperability brings benefits such as cooperation. It facilitates the exchange, sharing and reuse of information, thus improving the delivery of European public services to citizens and business, reducing costs and preventing duplication of efforts".

take over sectorial competences neither at EU nor at national level. It is aiming at facilitating the interconnection of these systems, building on already existing specifications and solutions.

While information stems from mainly public but also private sources, such as in the case of environmental data or weather forecasts, the exchange of information in the context of CISE is essentially meant for public authorities.Aggregated data such as future statistics on maritime occurrences potentially resulting from CISE information may nevertheless become public if deemed appropriate.

This is confirmed by Member States in the surveys, indicating that they see moderate to significant potentials for their surveillance tasks with better information sharing across sectors and across countries, given that their current systems will remain in place.
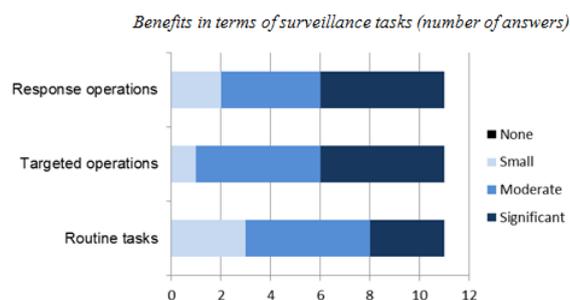

Figure 4- Benefits in terms of surveillance tasks (source: Member States survey)

5.2. Specific objectives

The **first specific objective** is to identify and address real or perceived legal limitations between sectors to justified exchange of maritime surveillance information and services Actions may include the development of a model Article to provide for a legal basis to information sharing between sectors. When personal data are exchanged, the requirements of the EU legal framework and relevant national legislation on the protection of personal data have to be respected. This means in practice that data can be exchanged inter alia if it is necessary, proportionate and appropriate to achieve the defined objective.

The **second specific objective** is to ensure interoperability between relevant IT solutions used by maritime surveillance actors through the use of common standards and specifications. This objective addresses the second cause of the problem identified under section 4.2. It addresses any remaining semantic and technical barriers to information exchange between sectoral functions, hence enabling easier, increased and seamless information sharing among maritime surveillance authorities. The objective will be to ensure that information can be transferred and incorporated into existing IT solutions without any manual data entry. The long term vision is that maritime surveillance IT providers one day implement and test IT solutions EU wide based on commonly agreed international standards[80]. It would mean allowing not only information exchange, but also exchanging knowledge through high value services. The exchange of structured information allows for automatic electronic information processing and data mining (e.g. for automatic anomalies detection).

European standards and standardisation are very effective policy tools for the EU. In particular the Digital Agenda for Europe highlights the importance of IT standards in delivering interoperability between devices, applications, data repositories, services and networks. The common data model ensuring semantic interoperability of information

---

[80] Similarly to what is happening in the eHealth sector with the IHE initiative (www.ihe.net) or in the eProcurement sector with the OpenPEPPOL Association (www.peppol.eu).

exchanges in maritime surveillance would be standardised with a recognised standardisation body[81]. The public consultation confirms the interest of exploring standards-based interoperability. The formalisation of such common data model for the IT industry would mean a significant reduction in its solutions' development cost in designing, production and sales phases, together with a consistent reduction of the industrial risks of missing return on investments. Introducing such standard would also lead to administrative simplification and reduction of administrative burden throughout the EU/EEA. Moreover the compliance with a unique and widely accepted set of standards at International or European level would raise the probability of acceptance by third countries.

The concrete result in the example referred to in section 4.2 would be that the maritime surveillance authority in Member State A can transmit the relevant information electronically and automatically between the IT systems of the two authorities without any manual intervention. The information would be available immediately for automatic processing or for human analysis by an operator and without any possible encoding errors. In addition, the same information can easily, if there is a justified need, be retransmitted to a connected maritime surveillance authority in Member State C and at low cost.

Standards needed in this respect would include the definition of a common data model (specifying consistent and agreed formats for electronic information exchange) and the definition of messaging protocols for trusted and secure information exchange.

Supporting tools to foster cooperation would also be needed: a register of maritime surveillance authorities in EU/EEA with their contact details, tools for virtual collaboration (e.g. videoconference), and a data dictionary to document and disseminate the agreed common data model.

Special software called 'reference implementation' would be put at the disposal of the Member States authorities to facilitate the interconnections. The principle is very similar to existing solutions, also working in decentralised environments[82]: the MEXS component distributed by the MARSUR to the participating defence authorities, the FLUX component distributed by the Commission to fisheries authorities to exchange i.a. VMS data, the EUROSUR nodes which facilitate the exchange of information between national border control authorities, the National Single Windows making available port reporting formalities to national maritime security and safety, customs, border control and health authorities or the e-TrustEx platform[83] which is available to any interested public authority in Europe for the secure digital exchange of documents.

It is unclear at this stage to what extent these solutions could be reused, as this will depend on the results of the Cooperation Project[84] from which more detailed requirements for CISE will be derived[85]. It is proposed to perform such detailed assessment when the results of the

---

[81]   In Europe, standards are developed and agreed by the three officially recognized European Standardization Organisations: the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI)

[82]   See study on Architecture Visions and existing systems at EU level for more information

[83]   The platform has been developed with the support of the ISA programme and is currently being tested in a pilot phase with several national authorities, the European Parliament, the Council and the Publication Office

[84]   The Cooperation Project Maritime Surveillance is a project run by 11 Member States and Norway, aiming at defining a set of useful cross-sector and cross-border information services, and at defining the needed supporting common data model

[85]   Several scenarios can be envisaged:

Cooperation Project are available in view of minimising the cost of implementing a reference implementation for CISE by reusing as much as possible from these solutions.

The **third specific objective** is to build confidence in order to bring maritime surveillance authorities of different sectors together and seek for better co-operation inter alia through joint missions, common operational procedures and training, best practices sharing etc. Experiences of co-operation within sectors and across sectors such as BLUEMASSMED and MARSUNO pilot projects[86+83] have shown that authorities are more at ease to co-operate and exchange information with each other when officials get to know each other through regular cooperation, etc.

6.   POLICY OPTIONS

6.1.   Selecting the policy options

A whole spectrum of possible options to ensure an optimum exchange of maritime surveillance information within and between sectors can be envisaged. Here, only those options that, prima facie, a) contribute to the objectives laid out in section 5, b) are legally feasible and c) do not entail disproportional costs for public administration, businesses and citizens, are retained for further analysis in sections 7 and 8.

6.2.   Discarded options

- A first option to consider would be to discontinue the current work at EU level, including funding of various pilot and co-operation programmes. Any further action to promote information exchange between different maritime surveillance sectors would be left to national authorities or individual sectors.

This option is immediately discarded as it would ignore the expectations of Member States and stakeholders to pursue action within the field of integrating maritime surveillance, as expressed in various council conclusions and ministerial declarations, and would fall considerably short of achieving the objectives identified in section 5.

- Should regulatory actions be considered, different levels of actions are possible. The most intrusive option would be to dismantle the existing sectorial information exchange systems and build a new system covering all sectors from scratch.

This option is immediately discarded as it would make no use of all efforts and investments made by different sectors during a long period of time to create functioning information exchange mechanism with their respective sectors. These systems have developed through time and are in general carefully crafted to strike a balance between different often conflicting interests. This option would also lead to a disproportionate workload for legislators and involved stakeholders compared to the expected benefits. In actual fact, it would delay the development of a common information sharing environment since all structures and organisational matters for existing structures would have to be renegotiated between interested parties. Such action is therefore very disproportionate compared to the defined objectives and would also disrespect the subsidiarity principle.

- Leverage the solution: the solution is performing well operationally, and is reported as compliant with CISE (as it is) and therefore it is ready to be reused.
- Convert the solution: The solution is performing operationally well, but additional investment is required to make it CISE compliant and then reuse it across the board.
- Reuse parts of the solution: The solution can provide input to CISE reference implementation which will in any case be something new.

86   See footnotes n°23 and n°24

Any option which is not built on current achievements and existing sector systems is therefore immediately discarded.

- Another option would have been to seek amendments of horizontal EU legislation in force or in coming which are imposing certain conditions for the transmission of certain related information, such as rules on transparency and the protection of personal or commercial data

Such an option can also be immediately disregarded since the objective of this initiative by no means is to review provisions of that nature. In other words, this initiative should not lead to any amendments to the future personal data protection package. For this reason, no option which would lead to free flow of confidential (personal or commercially sensitive data) information can be retained.

6.3. Retained policy options

The policy options retained for a more in depth analysis can broadly be divided into three different categories:

- No further EU action;

- Voluntary measures; and

- Legally binding measures.

6.3.1. Option 1- No further EU action

No policy Change (baseline scenario)

Until now, no specific legislative initiatives have been taken to implement the CISE project. The Commission has so far issued two Communications to define the aim of the CISE project, identify the guiding principles and steps towards its establishment. Along with various EU funded pilot projects, these initiatives have already contributed to raising the awareness among national maritime surveillance authorities of the importance and necessity to share maritime surveillance information and inspired some initiatives among certain sectors.. For example, as already highlighted above, the implementation of "national single windows", as required by Directive 2010/65/EU, is envisaging sharing of information to other sectors on national and EU level. This is also the case for the fisheries control Regulation[87+84].

This option would mean that EU interventions continue as before and that no specific instrument is developed at EU level. In substance, EU interventions would focus on facilitating a dialogue between stakeholders through Member State Expert Groups and other similar bodies created with the aim to enhance dialogue and co-operation between sectors.

Another important aspect would be to provide continued funding to various projects. Regulation (EU) n°1255/2011[88+85] has already provided funding for CISE related projects during 2011-2013. Funding for future projects for the 2014-2020 period are currently under negotiation with the legislative bodies in the Regulation for the future European maritime affaires and fisheries fund (EMFF).

Under this option the future development of the CISE project would to a large extent depend on Member States and sector initiatives to obtain interoperability of the existing maritime surveillance information sharing systems. The role of the EU would be limited to foster

---

[87]   Directive and Regulations referred to above.

[88]   Regulation (EU) No 1255/2011 of the European Parliament and of the Council of 30 November 2011 establishing a Programme to support the further development of an Integrated Maritime Policy.

dialogue between different stakeholders. No EU interoperability standard would be pursued. This policy option has received very limited support from stakeholders.

6.3.2. *Option 2 -Voluntary measures*

This option contains various sub-options with a higher ambition level and could provide a more stringent framework compared to the previous option. It could also help co-ordinating efforts between maritime surveillance authorities and sectors. This is the policy option which attracts the most support among stakeholders.

The success of the voluntary measures would still depend on the willingness of the different actors to participate, but may provide responsiveness and flexibility.

This policy option can be divided into the following sub-options:

6.3.2.1. Establishment of a Communication

In substance, the purpose of This Communication would be to take stock of the current situation, review the the 2010 roadmap , assess the added value of enhanced information exchange and the need for further EU action, further clarify the respective roles of the EU and its Member States, identify priority areas for further intervention at EU level and to propose and updated roadmap and provide a roadmap for the next steps..

In particular, the Communication should identify:

- The actions which the Commission considers should be taken to address any legal, technical and cultural limitations to the exchange of information services between maritime surveillance authorities. This with a view to promote a dare to share culture and to provide Member States with the appropriate references to take the necessary aciton at national level.

- The current interoperability solutions, the interoperability convergence to be achieved in the medium term and the EU wide interoperability standards needed in the long term. This with a view to allowing Member States, the European Commission, and where necessary in cooperation with industrial players, to elaborate the most appropriate long term interoperability framework for the EU with the objective of ensuring the interoperability of maritime surveillance systems.

- By which means co-operation between civilian and military authorities can be enhanced.

- Means to strengthen the fundamental rights of citizens by bringing guidance on how information exchange need to be arranged while respecting the EU charter on fundamental rights and data protection rules at national and EU level.

The objective would be to create an opportunity to have a more in depth discussion with the co-legislators and stakeholders on how to implement the CISE project and to have a common understanding on the next steps to take. The objective is not to promote the creation of any new obligations to collect data, but rather to move from a single purpose use to a multipurpose use of already collected data and thus reduce duplication of data collection efforts.

6.3.2.2. Establishment of soft policy initiatives such as a guidance document and best practices

This sub-option consists in developing a guidance document or a handbook for the further development and functioning of CISE. This process should be steered by the Commission and the document should be elaborated in close contact with Member States experts. This

document may provide recommendations, guidelines and best practices on information sharing. The purpose would be encouraging increased cooperation among EU Member State authorities on a voluntary basis to address cultural barriers. This document should be developed outside any legislative process in order to ensure the uptake of all relevant stakeholders and to be able to address enhanced information exchange between civilian and military authorities.

In substance, such a document may contain:

- Key definition of the most important concepts;

- Key guiding principles for information sharing including governance and responsibility to share surveillance information with other sectors in line with EU on the protection of personal data;

- Key recommendations on legal, technical and operational matters for information sharing such as:

- Suggestions to Member States' maritime surveillance authorities as how they can go about to exchange information across-borders and across-sectors, including using a common data dictionary and common technical standards allowing for the interoperability of the surveillance systems of different sectors; as well as how to deal with perceived or real legal limitations at national level.

- Administrative practice in a coordinated manner by providing guidelines in order to help Member States and other stakeholders to interpret and apply specific provisions of EU legislation. This may, in turn stimulate changes in national legislation in situations, when it contains provisions which are more stringent in comparison with the legislation on EU level;

- A description of core information services and standardised form for the conclusion of agreements (Memorandums of Understanding and Service Level Agreements) among the Member State maritime surveillance authorities and EU agencies regarding the conditions for information sharing and the use of the data shared; and

- Available or possible IT standards for interoperability, possibly elaborated through a standardisation body as referred to in section 5.2. To do this, the Commission will explore the feasibility of develop common standards through the established processes at EU level, ensuring a strong involvement of Member States through their national standardisation bodies.

6.3.2.3. Establishment of a joint undertaking pursuant to Article 187 of the TFEU

The voluntary approach may be formally founded on a joint undertaking. Such undertaking may provide a framework for further activities, encourage and, when appropriate, assist EU Member States to increase maritime surveillance information sharing among sectoral functions and to achieve a more effective and coordinated information sharing. A joint undertaking is typically established by a Council Regulation. Such Regulation is adopted on a proposal from the Commission and after consulting the European Parliament and the Economic and Social Committee, relying on the legal basis in Article 187 TFEU. In the case of CISE a joint undertaking may foster research on interoperability, on new future-oriented maritime surveillance information services and on civil-military cooperation.

In substance, the objective of this sub-option would be to address the same issues as those referred to in the previous sub-option.

This option would be relevant when a temporary framework for the establishment of the CISE project would be useful and can provide a flexible mechanism for further cooperation.

6.3.3. *Option 3 -Binding measures*

This policy option seeks to implement the objectives of the CISE project through a legally binding approach. It thus constitutes a further upgrade of the ambition level compared to the previous option. Any such legislative proposal would be accompanied with an impact assessment, which would also identify the process involved depending of the circumstances of each legislative instrument and to what extent for example such changes would be the subject matter for delegated or implementing acts. This policy option has received a mixed reaction from stakeholders. While some are keen to see binding measures in place, the bigger majority feels that binding measures are not necessary. It includes the following sub-options:

6.3.3.1. Establishment of a policy package within the existing legislative framework

The purpose of this sub-option would be to envisage amendments, if necessary, of existing sector EU rules regulating information exchange of maritime surveillance related information. It does not envisage the adoption of a new instrument at EU level, nor address legal limitations at national level. An inventory of the existing legislative framework has shown that most if not all legal limitations at EU level have already been removed or are in the process of being removed. There can however be different interpretations to what extent a specific rule constitutes a legal limitation or is justified and put in place for reasons of data protection.

In substance, the main objective of this sub-option would be to address identified legal limitations in sector legislation to cross-border and cross-sector information sharing and to complement existing standards for information exchange with interoperability standards between sector systems through delegated or implementing acts.

The revision of these provisions will also confirm the same level of conditions for access so that all sectors which have a justified need to receive certain maritime surveillance information indeed can do so. These revised provisions will have to be accompanied by the same safeguards in accordance with the principles of protection of the fundamental rights of an individual and confidentiality as is already in place for the data exchanges within sectors.

It is envisaged that the amending acts will rely on the existing sector mandates of the TFEU and include an explicit delegation to the Commission (Art. 290 TFEU) to supplement certain non-essential elements of the amended act to, in particular, overcome technical barriers.

6.3.3.2. Establishment of a cross sector legislative framework on CISE (Regulation)

The main objective of this sub-option would be to put in place a legally binding legislative framework which would not only seek to address the legal limitations and introduce technical interoperability standards of the previous sub-option, but also put in place other building blocks of the CISE in a binding fashion.

In substance, such a Regulation could contain for example:

- Key definition of the most important concepts;

- Guiding principles for the running of CISE for a multi sectorial functions;

- Establishment of key governance principles for the running of CISE;

- Key obligations on responsibility to share surveillance information to other sectors;

- Provisions on reporting and monitoring; and

- Provisions for the adoption of delegated/implementing acts. The purpose of these acts would mainly be to allow for the establishment of common technical standards allowing for the interoperability of sector surveillance systems.

As noted above (see section legal basis), such a framework would be split into several umbrella packages depending on the legal basis, applicable legislative procedures, and constitutional opt-in and opt-outs from the EU Treaties. In order to maintain a cross sector approach, it would rely on a multiple legal basis. It would only cover sectors covered by the EU Treaties and would therefore exclude the defence sector.

6.3.3.3. Establishment of a cross sector legislative framework for the technical aspects of CISE

This sub-option can be described as a combination of the two sub-options for a binding legislative framework described above. It would essentially be a technical regulation which in substance would be putting in place the necessary interoperability standards for EU wide exchange of information services. This would be a European Standard for a common data model. This approach would be relatively similar to the approach taken for the Inspire Directive[40].

6.3.4. Combination of policy options

A combination of some of the different policy option outlined above is also possible. This is likely to occur in this particular case since it is not likely that one option or sub-option will prove successful to obtain all the objectives defined in section 5.

7. ASSESSMENT OF OPTIONS

The assessment of the different policy options will be made in the following four steps:

- A <u>qualitative</u> assessment of each policy option. The purpose of this assessment will be to examine the effectiveness and efficiency in meeting the objectives defined in section 5 on the one hand, and the degree of coherence with the objectives of existing EU policies, such as the Integrate maritime policy of the EU and the sector policies of the seven sectoral functions dealing with maritime surveillance, on the other, compared with the baseline scenario.

- A <u>quantitative</u> assessment of the potential added value of each policy option and of the development of the full potential of a Common Information Sharing Environment as such. The purpose of this assessment will be to examine the economic, social and environmental benefits compared to the baseline scenario.

- An assessment of the impacts of these options on fundamental rights.

- An assessment of <u>cost</u>. The purpose of this assessment will be to examine both the expected cost for each policy option and for the development of CISE as such for putting in place an interoperability framework compared to the baseline scenario.

There are two main reasons why this methodology has been chosen:

First of all, the nature of the topic is such that the conditions from making a quantitative assessment of each option are quite different from making a qualitative assessment. While the

qualitative assessment can be relatively straightforward, the quantitative assessment is quite a challenge.

The main reason for this is that the main benefit for enhanced information sharing, namely better governance, is very difficult to evaluate in quantitative terms. Attempts have been made to evaluate such benefits both in the consultancy studies and preparatory actions in support of this impact assessment, but those attempts, although involving Member States as actors, can at the end of the day only consist of range estimations of what such quantitative benefits could be. For some elements however, such as reduction of duplication in data collection efforts and reduced costs for patrol activities, a more precise estimation has been possible.

Secondly, while the initiative is expected to have benefits on the EU economy, society and environment, it has not been possible to make a well-reasoned and convincing distinction between the potential economic, social and environmental impacts of each policy option. This is because this policy initiative essentially is about ensuring better interoperability between the different information exchange systems of different sectorial functions that together ensure economic, social and environmental benefits. The initiative is in other words almost exclusively about enhancing technologies and resource efficiency, which can lead to more effective and cost efficient maritime surveillance activities. Thus, the economic, social and environmental impact of such interoperability initiative cannot be distinguished for each policy option. Therefore the quantitative assessment will compare the combined economic, social and environmental benefits of each policy option with the full CISE potential.

7.1. Qualitative assessment of options

7.1.1. Option 1 – No EU action (baseline scenario)

Effectiveness

This option can contribute to achieving some of the objectives in section 5 through the existing cross sector dialogue and through the funding of projects via the EMFF Regulation. The launch of the CISE initiative in 2007 has indeed, as highlighted above lead to some success stories and fostered enhanced dialogue between different maritime surveillance sectors and this positive progress can continue if this dialogue is pursued. This option could also help removing some cultural barriers.

However, this option would not address any legal limitations or technical barriers identified and would not lead to any co-ordinated action at EU level. The 2010 CISE Roadmap would continue to be implemented, but in a non-coherent manner. This option would also fall short of the expectations of legislative bodies and stakeholders referred to in section 3, whereby it is requested that EU steps up its action on this initiative to implement the objective defined in section 5. Some Member States are as well presently waiting for EU common interoperability solutions to adapt their own maritime surveillance systems. It is also unlikely that enhanced information exchange between civilian and military authorities can be fostered specifically further.

The baseline (no specific EU action) would mean that individual sectors at EU level carry out their current and planned policies in such a way that it leads to a certain level of cross-sectorial interoperability. However, such sectorial initiatives do not tackle a number of essential CISE features:

i.) the various sectorial interoperability solutions, stand-alone those at EU level related e.g. to the National Single Window, Eurosur, Flux, Marsur, Siena, e-Customs, SEIS and CECIS are not designed to be mutually interoperable;

ii.) individual sectors have so far shown little ability to seek for coherent overarching cross-sectorial interoperability solutions that integrate into the EU's overarching interoperability framework;

iii.) sectorial EU interoperability solutions do not provide for connections between national authorities across sectors and borders: coast guards or national maritime surveillance centres have the need to correlate data for building intelligence, awareness and knowledge; if they receive various data in various formats and standards from various surveillance functions in various Member States and from various EU Agencies, correlation and intelligence building remains difficult and thus ineffective. The reason for this being that without overarching coherent interoperability, data can still not be integrated in an efficient, cost effective and coherent manner into the operator's own system and preferably on a single screen, due to a lack of semantic, organisational, technical, legal and political interoperability, and finally,

iv.) sectorial EU interoperability solutions will not allow for the sufficient 'point to point' interoperability between relevant national authorities of any type to develop and exchange new information services allowing e.g. various coast guards functions to coordinate their operations and assets even if they are distributed within various areas of competence.

Enhanced dialogue will continue to lead to certain benefits, but there is a risk that with a low level of ambition that this option represents, stakeholders will lose interest in the topic with the result that no flexible, efficient, cost effective and coherent solution can be found to satisfy Member States' needs.

Coherence

This option will contribute to better coherence of sectorial policies provided that the progress towards better information exchange that has been achieved between 2007 and 2013 continues in the future in line with the objectives of the IMP. However, coherence between policies is likely to be suboptimal in the absence of any structured regime. Unless these issues are being discussed together by the different sector with a view to achieve common solution, incoherencies between different sector policies risk to persist.

7.1.2. Option 2 – Voluntary measures

7.1.2.1. Communication

Effectiveness

As such a Communication can contribute to achieve some of the non-regulatory issues defined in the objectives through enhanced dialogue with the relevant stakeholders, and would put the subject matter higher on the political agenda. However, this option will not as such

address any legal limitations or technical barriers identified other than to identify options for solving these issues at a later stage or through separate measures.

A Communication could however be a very useful tool to establish priorities, distinguish action at EU and national level, set out short, mid and long term implementing roadmap towards progressively building up overarching, effective, cost-efficient and fully coherent interoperability solutions.

Finally, a Communication could inject further ideas for enhanced information exchange between civilian and military authorities and could in fact be one of the most effective means to foster a dialogue in this respect. Provided that this instrument can provide for such a roadmap, the effectiveness would be higher than the baseline scenario.

Coherence

This option can, through enhanced dialogue, contribute to better coherence of data exchange systems within the field of maritime surveillance in line with the Integrated Maritime Policy. The effect is however uncertain since progress at the end of the day will depend on the willingness of the stakeholders to take part in that dialogue. However, if constructed as a roadmap from short to long terms, the results are likely to be positive since the latter allows for a progressive process towards developing and implementing the required interoperability solutions of the future while departing from the on-going developments and allowing all stakeholders to take active part in the process. A Communication taking account of short, mid and long term opportunities will therefore provide a higher degree of coherence compared to the baseline.

7.1.2.2. Guidelines and best practices

Effectiveness

Providing a guidance document with best practices could be a very useful tool to achieve the objectives identified, in particular the removal of cultural barriers. It is clear that many aspects of the CISE project neither can nor should be the subject matter of any form of legal or legislative act, among other reasons due to the decentralised character of the operative data exchanges. An operative guideline which in very concrete terms addresses some of the most common issues that maritime surveillance authorities are confronted with at operative level and provides for best practices should be drafted in close collaboration with the technical experts at Member State level and could considerably help in obtaining a common understanding on practical matters and the operational needs.

Such an approach will also partially address the expectations of stakeholders. It will however not as such address any remaining legal limitations or technical barriers, although it can help dismantle and clarify certain issues which are wrongfully perceived as being legal limitations or technical barriers (such as personal data protection issues).

A biggest advantage of this option would be that it would provide a clearer framework for the CISE initiative and would provide a suitable degree of flexibility for the actors concerned as to the practicalities. A clear advantage would be that such guidelines would be a sufficiently flexible instrument to address the need for enhanced information exchange between civilian and military authorities.

The effectiveness of this option is therefore likely to be considerably higher compared to the baseline.

Coherence

This option will contribute in a better way than previous options to a better coherence and integration of sector policy work in line with the IMP. Working closer with officials of other sectors and bringing in all the expertise at Member States level will also help breaking down distrust and invisible barriers and contribute to a dare to share environment.

Another positive aspect with this option is it will institutionalise the objectives of more integrated information exchange between sectors in a non-binding legal act. The effectiveness is however uncertain due to the voluntary nature of the instrument.

7.1.2.3. Joint undertaking

Effectiveness

The advantage of a joint undertaking is the flexibility such arrangement offers; this includes the scope, governance, funding (regarding both the Member States and EU's contribution) and the duration of the undertaking. It would also allow defining the individual members' roles in specific agreements, which may be for that purpose concluded with the joint undertaking. This would allow taking into account specific Member States national prerogatives or other interests both at the Member States and sectorial function level. The formal functioning of the undertaking would be governed by the undertaking's internal statutes, which could be amended according to the procedure agreed between the undertaking's members. A joint undertaking could allow for a formal agreement between the signing parties to proceed with sharing of information and collaboration in addition to what is already foreseen at the present time. In any case, it would have the potential of stimulating cross-sectorial and cross-border information sharing in the areas where the sharing of information is not legally excluded.

This policy option may be perceived as a step in the overall CISE development; contributing, on the one hand, to overcoming cultural barriers and, on the other hand, providing a basis for future legislative changes. It will however not address any legal limitations and technical barriers as such, but can contribute considerably to enhance information exchange between civilian and military authorities.

The main disadvantage of this option is that it does not constitute a light approach. A joint undertaking requires that a whole structure is put in place, including a secretariat. There is in other words a risk that this option will make use of considerable resources in putting the undertaking in place, which risk further delaying the implementation of the objectives defined in section 5. It is also uncertain if this instrument can be used at all to address legal limitations since joint undertakings normally have a strong research and technical angle.

In conclusion, this option is likely to be more effective in a medium term to implement the objectives compared to the baseline scenario.

Coherence

This option is likely to contribute significantly to the coherence of sector policies since it will ensure a formal set up for the dialogue. It is however uncertain that this option will lead to better coherence of sector policies further downstream compared to the baseline if the joint undertaking is not supported by any concrete policy measures.

7.1.3.   Option 3 – Binding measures

7.1.3.1. Amendments of sector legislations

Effectiveness

This option is likely to address some of the objectives in a much more efficient way than the baseline scenario. Only binding options can address any the legal limitations and technical barriers identified, since these are laid down in different legislative acts. A clear advantage with this option is that it follows the legislative approach of the TFEU which provides the legal basis sector by sector. A review and revision process within the current legislative framework which could lead to a clear mandate (legal basis) for cross sector information exchange will ensure coherence with existing obligations within sectors and can also make use of existing provisions of relevance such as provisions on access to data and confidentiality. This option can also provide for common standards for interoperability and thus solve technical barriers.

This option can however not address cultural barriers and other non-legislative building blocks of CISE such as operational and confidence building issues. Nor will it address the need for better information exchange between civilian and military authorities.

Coherence

This option is likely to be effective in ensuring coherence between sector policies since issues will be covered in a regulatory framework. The need to co-operate between sectors will be fully recognised in EU legislation to the gain for integration. This can be achieved through a process whereby the amending rules are co-ordinated with each other to be ensured that no incoherencies or inconsistencies are created.

7.1.3.2. A cross sector Regulation

Effectiveness

This option could in normal cases be considered as the best possible option since it basically could cover all the fundamental aspects of the CISE project. Not only does it provide for a solution to address legal limitations and technical barriers, but it could also address certain cultural barriers through the adoption of guiding principles etc.

However, this option could entail a high level of complexity given the ambition to cover information exchange between seven sectors, which do not have the same procedures for legislative action and for some instances are not even covered in the same Treaty. This means that several similar Regulations will have to be adopted. In order to achieve a neutral balance between sector interests, such instrument would have to be adopted with a multiple legal basis in line with current developments of the IMP and be complemented by additional legislation

covering the Title V of the TFEU. It could be regarded as too intrusive by stakeholders and can only address cultural barriers in a limited way due to subsidiarity issues.

EU legislative measures may not include navies as they fall outside TFEU and are only subject to TEU to a limited extent.

Therefore, this option is not likely to be in the short term more effective in implementing the objectives compared to the baseline scenario. Nor will it address the need for better information exchange between civilian and military authorities. However, if in the mid to long term stakeholders develop a common understanding on which interoperability solutions best suit them it might then be effective to implement such solutions by means of a cross- sectorial Regulation in the long term. The legal complexity of this option will however remain.

Coherence

In the short term it is perceived that the existing maritime surveillance landscape is too complex for fully coherent interoperability solutions to be implemented by a cross-sectorial Regulation. In the long term however, if stakeholders may develop a common understanding of what is needed, a cross-sectorial Regulation may indeed have the potential to provide for the sought coherence.

7.1.3.3. Technical Regulation

Effectiveness

This option is likely to be more effective in implementing the objectives than both the baseline scenario and the previous option for cross sector legislation. Although this option may suffer from the same complexities as the previous option, it would constitute a more smooth option that focuses on the topics where binding measures could have considerable benefits. In conclusion, this option is likely to be more effective in a long term to implement the objectives compared to the baseline scenario.

Coherence

The same considerations on coherency apply for this option as for the previous option.

7.2. Quantitative assessment

7.2.1. Economic, social and environmental impacts of implementing the CISE project

The overall impact (benefit) of CISE is estimated to range between 160 million €per year and 420 million €per year over ten years as from the moment CISE is in place[89].

This calculation is based on estimates by national maritime surveillance experts engaged in preparatory actions as well as studies referred to in Section 3.

The overall methodology chosen was to compare the effectiveness and cost efficiency of maritime surveillance today (without CISE) in accordance with the baseline scenario with a scenario if CISE would be fully in place.

---

[89]   CISE in place: All limitations to information sharing (legal, technical and cultural limitations and barriers) have been addressed and a significant part of the information gap identified by TAG is closed.

Three different sources of economic data were used: First, the macro data collected from Member States through the Member States expert group (MSEsG), second, the detailed cost and benefit data collected from Member States active in preparatory actions (TAG and the CISE Cooperation project) and third, economic and impact statistics on maritime phenomena at European and international level.

This logic was deployed both through a *bottom-up* and a *top-down* approach with a risk analysis.

The Bottom-up approach consisted in selecting a representative sample of relevant maritime surveillance 'success' indicators such as the reduction of goods being smuggled into the EU (e.g. arms and light weapons), of oil pollutions at sea, of illegal unregulated and unreported (IUU) fisheries, of accidents at sea, of human trafficking, of piracy and most importantly, succeeding in saving more lives at sea. Then a series of representative real life scenarios were drawn up of *routine*, *semi routine* and *exceptional* maritime surveillance actions (use cases) as typically carried out by Coast Guard functions representing all seven functions involved in maritime surveillance. These use cases were then used to compare the situation today (baseline) with a scenario if CISE would be fully operational (CISE full potential).

The resulting added value of CISE measured in terms of improved 'success' rate of the above indicators, was then used to calculate the wider impacts corresponding to the individual 'success indicators'. This was done based on available statistics from e.g. Eurostat, OECD and other recognised sources.

The Top-down approach consisted in an estimate of overall maritime surveillance cost today for certain Member States. These estimates were put in context of size and importance of the countries selected and their spending on maritime surveillance activities. The results of this top-down approach matched those of the bottom-up approach.

The risk analysis consisted in an analysis of challenges, risks, threats and vulnerabilities on the world wide maritime areas of interest to Europe (including the Baltic, the North Celtic Sea, Biscay/Iberia, Black Sea, Mediterranean, Arctic Ocean, Oversees and High Seas). This analysis concluded that enhancing knowledge and improving maritime situational awareness could potentially lead to the reduction of threats and risks by about 30% on average[90], while this effect will of course not be uniform over the type of risk and the different maritime areas of European interest.

The result of the above analysis was then compared with the various policy options, with the view in particular to determine the extent to which each individual option may reach the full CISE potential.

---

[90]   To be more precise, 'risks' as referred to above are understood as being a combination of 'risks' and their 'impacts'. Depending on the sea basin and the situation one may encounter a combination of 'high risk' with 'low impact' or vice versa. The resulting combination of risks and their impacts may be referred to as level of 'danger'. It is such level of danger that is being reduced by 30% in average. For simplicity however the present text only refers to (threats and) risks being reduced by 30% through enhanced knowledge and improved maritime situational awareness.

7.2.2.   Economic, social and environmental impacts of each Policy option

7.2.2.1. Option 1 – No EU action (baseline scenario)

The 'baseline' is the reference departure point for all other options.
As a consequence, being the reference departure point for all other options its 'additional' value added has been considered to be zero for normative reasons. This allows all other policy options to be compared to the baseline.

7.2.2.2. Option 2 - Voluntary measures

Communication

The benefits of this option are likely to be similar to the baseline scenario but will be higher if in very concrete terms it identifies the necessary measures to be taken to achieve the defined objectives. The benefits will stem from the concrete actions taken at a later stage.

As a consequence, it is estimated that compared to the baseline, this sub-option (stand-alone) may realise 20 % of the full potential of the CISE project, while incurring 60 M€ Total Ownership Cost (TCO), realising 37 M€ cost savings, 114 M€ beneficial impact and may thus realise at least a progressively cumulated[91] positive impact of 151 M€ over the first ten years during which CISE is being progressively set up.

Guidelines and best practices through a Recommendation

The benefits of this option are likely to be significant compared with the baseline scenario because it can more effectively address the cultural barriers and clarify misconceptions. It could thus directly promote and enable such information exchanges which do not require the removal of technical barriers or legal limitations and can therefore lead to quite quantifiable benefits compared to the baseline. Better co-operation between stakeholders of different sectors is likely to contribute to efficiency gains and reduced costs for administration.

As a consequence, it is estimated that compared to the baseline, this sub-option (stand-alone) may realise 40 % of the full potential of the CISE project, while incurring 75 M€ TCO, realising 75 M€ cost savings, 228 M€ beneficial impact and may thus realise at least a progressively cumulated positive impact of 303 M€ over the first ten years during which CISE is being progressively set up.

Joint undertaking

The benefits of this option are likely to be considerable compared with the previous option and high compared to the baseline as the joint undertaking provides a forum in which all stakeholders at EU and national level as well as industry may be represented to commonly elaborate what *they* need. This option could thus provide an inclusive approach towards maritime surveillance practitioners and is thus considered to have a high uptake of the CISE full potential. There is however a risk that the benefits would be reduced or occur more downstream if it turns out that the administrative process for setting up the joint undertaking turns out to be complex.

---

[91]   It is understood that CISE will be established step by step and that the benefit would thus increase proportionally over the first ten years.

As a consequence, it is estimated that, compared to the baseline, this sub-option (stand-alone) may realise 65 % of the full potential of the CISE project, while incurring 106 M€ TCO, realising 122 M€ cost savings, 373 M€ beneficial impact and may thus realise at least a progressively cumulated positive impact of 495 M€ over the first ten years during which CISE is being progressively set up.

7.2.2.3. Option 3 – Binding measures

Amendments of sector legislations

The benefits are a priori likely to be significant under this option compared to the baseline since it is meant to address legal limitations and provide a solid mandate (legal basis) for information exchange between sectors. The introduction of more automated information exchanges will also lead to considerable cost savings with the introduction of technical interoperability standards. A more coherent information exchange system at EU level will also lead to efficiency gains downstream through closer collaboration between maritime surveillance authorities.

As a consequence, it is estimated that, compared to the baseline, this sub-option (stand-alone) may realise 50 % of the full potential of the CISE project, while incurring 86 M€ TCO realising 94 M€ cost savings, 286 M€ beneficial impact and may thus realise at least a progressively cumulated positive impact of 380 M€ over the first ten years during which CISE is being progressively set up.

Cross sector Regulation

While this option would *a priori* allow for effective application of interoperability solutions, it is however unlikely that in the short term a one fits all solution can be found considering the complexity arising from the diversity and the great number of stakeholders with many different systems having miscellaneous needs and various organisational structures. In the *short term* authorities at EU and national level:

i.)   Are unlikely to adhere to an imposed solution likely to incur a high administrative burden while they may not need or want this solution and

ii.)   Have expressed their need for cheap, easy to implement and fully flexible decentralised interoperability solution allowing them to doing what fits them best.

As a consequence, it is estimated that, compared to the baseline, this sub-option (stand-alone) may realise 50 % of the full potential of the CISE project, while incurring 86 M€ TCO realising 94 M€ cost savings, 286 M€ beneficial impact and may thus realise at least a progressively cumulated positive impact of 380 M€ over the first ten years during which CISE is being progressively set up. However, if in the mid to *long term* stakeholders develop a common understanding on which interoperability solutions best suit them it might then be effective to implement such solutions by means of a cross- sectorial Regulation in the long term. The uptake might then increase well beyond the indicated 50%.

Technical Regulation

The benefits of this option are likely to be equal to the previous option as such Regulation may allow to set an overarching reference standard for maritime surveillance interoperability that integrates with EU wide solutions. It can be expected that these benefits will occur more upstream compared to the previous option since the legislative process for putting such a Regulation will be less complicated, but will nevertheless require some time and effort. The main benefit with this option is that it will lead to more automatic information exchanges without human intervention allowing increased and faster information services exchanges and fostering data mining i.e. automatic or semi-automatic analysis of large quantities of data to extract e.g. unknown and interesting patterns to detect anomalies. While being more difficult to realise in the short term, this option may however be effective and coherent in the mid to long term.

As a consequence, it is estimated that, compared to the baseline, this sub-option (stand-alone) may realise 50 % of the full potential of the CISE project, while incurring 86 M€ TCO realising 94 M€ cost savings, 286 M€ beneficial impact and may thus realise at least a progressively cumulated positive impact of 380 M€ over the first ten years during which CISE is being progressively set up.

The following table provides an overview of the quantitative assessment the next ten years:

	Option 1: No EU action	Option 2.1: Communication	Option 2.2: Guidance document and best practices	Option 2.3: Joint undertaking	Option 3.1: Policy package within existing legislative framework	Option 3.2: Cross sector legislative framework on CISE (Regulation)	Option 3.3: Cross sector legislative framework for the technical aspects	Policy mix 2.1 + 2.2 + 3.1
Assumed realisation potential of full CISE benefit	**0%**	**20%**	**40%**	**65%**	**50%**	**50%**	**50%**	**80%**
Key measures (MEUR)								
TCO	**0**	**60**	**75**	**106**	**86**	**86**	**86**	**133**
Cost Savings	0	37	75	122	94	94	94	151
Impacts	0	114	228	373	286	286	286	460
Total benefit[92]	0	151	303	495	380	380	380	611
Performance ratios								
Cost savings/TCO	0	0.62	1.00	1.15	1.09	1.09	1.09	1.14
Impact /TCO	0	1.88	3.05	3.51	3.34	3.34	3.34	3.47
Total benefit/TCO	0	2.50	4.05	4.65	4.43	4.43	4.43	4.61

Table 1- Overview of the quantitative assessment (source: COWI study)

---

[92] As the implementation of CISE is an ongoing process and is intended to be implemented gradually, the 80% uptake of the full potential is meant to be reached after a progressive uptake over the next ten years. The gradually cumulated total benefit over the next ten years is thus less than 80% of the full potential (that may be assumed for the second ten year period).

Option 2.3 is the most costly option but it is also the option that delivers the highest expected benefits. The cost of Option 2.1 and 2.2 are relatively low but their level of individually reaching the CISE full potential is also relatively low. Option 3.1 aligns with Options 3.2 and 3.3 on cost and uptake of the CISE full potential, but are not convincing in the short term. A policy mix of Options 2.1, 2.2 and 3.1 is however expected to have the highest uptake of the full CISE potential in the short to mid-term while having an interesting benefit over cost ratio.

Indeed, elaborating a Communication and combine it with a Guidance document in the short term (elaborated in close co-operation with stakeholders at Member State level) and envisage reinforcements of sectorial legislation at EU level during the ordinary review process, would be the most appropriate means to achieve the objectives defined in section 5 in the short to medium term. This is the best solution, in particular as it allows for civil/military cooperation as from the short term.

7.3.   Assessment of impacts on fundamental rights

This policy initiative is relevant for the EU charter on Fundamental Rights, in essence its Article 8 regarding the protection of personal data. Thus, it has to be checked in detail whether additional processing operations (such as transfers of personal data to other surveillance authorities) are in accordance with law, pursues a legitimate purpose, is necessary in a democratic society, and in particular if it's proportionate to the legitimate aim pursued and if the reasons are relevant and sufficient. The core principles of data protection include the obligation of respecting purpose limitations with regard to new processing operations. These requirements are binding even though the receivers of the relevant data is limited to maritime surveillance authorities and is not intended for the wider public.

As noted above, the creation of a Common Information Sharing Environment for the EU maritime domain (CISE) is an on-going process which has already lead to certain success stories and lead to enhanced information exchange between maritime surveillance authorities. This process has and will be coupled with a fundamental rights assessment, in particular whenever legislative changes are made, to ensure that these rights are respected and that strict safeguards are in place when personal data is exchanged in accordance with EU and national law on the protection of personal data.

In case binding measures will be needed at a later stage, a further fundamental rights assessment will have to be included in the impact assessment of the relevant legislative proposal.

7.4.   Assessment of Cost and administrative burden

7.4.1.   Costs of the policy options

The purpose of this assessment will be to evaluate the direct investment cost of the Member States and at EU level to put in place the Common Information Sharing Environment[93].

The cost of implementing CISE depends to a large extent on how each Member State may want to organise itself internally to connect to the environment and the number of information services that will be provided in the environment. Another important element to take into

---

[93]   None of the policy options impose information reporting obligations. The impact of increased operational information exchanges on resources at Member States level has been included in the costing estimates.

consideration is that existing and planned systems that a common information sharing environment has to be built upon have developed at various speeds and reached different levels of maturity.

Preparatory actions have identified core IT components for facilitating information exchanges based on pre-defined principles and requirements and have compared different organisational approaches to the integration of information from seven different sectoral functions in the 28 EU Member States[94]. The comparison shows that the total costs[95] of CISE on a ten year period ranges from 83M€ to 142M€ for an arbitrary level of information exchanges compared to the full data gap identified under the baseline scenario. The cost analysis is based on a costing model which contains a set of assumptions (mainly IT related). These assumptions related mainly to the building blocks that are necessary to have an operational CISE. For example, the number of participants has been estimated, the level of information exchanges, the cost of software, the higher cost involved to connect older technologies in the Member States and the potential of reusing generic building blocks versus redevelopment by Member States. The complete set of assumptions can be found in the supporting study[96].

An organisational structure where Member States would set up central IT systems for information exchange related to maritime surveillance shows the lowest cost of realisation of 83M€ It is however more intrusive into the national structures and thus less recommendable and does not take into account the very diverse situation and the investment cycles in the Member States.

It is therefore proposed not to impose any governance structure to the Member States and let Member States connect their IT systems per sectoral functions to CISE. The cost of such an organisational structure is estimated at 107 M€ As said above, the number of information services that will be provided in the environment influences the total cost, which might vary from that total of 107 M€ The expected level of information exchanges varies depending on the policy option. The table below shows the cost of each policy option, with the corresponding expected level of information exchange compared to the full gap identified under the baseline scenario, and with the assumed realisation of full CISE benefits.

	Option 2.1: Communication	Option 2.2: Guidance document and best practices	Option 2.3: Joint undertaking	Option 3.1: Policy package within existing legislative framework	Option 3.2: Cross sector legislative framework on CISE (Regulation)	Option 3.3: Cross sector legislative framework for the technical aspects
% data sharing versus baseline	4%	16%	42%	28%	28%	28%

---

[94] See Commission study on CISE Architecture Visions and existing systems at EU level for more information, available on
http://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance/index_en.htm

[95] The total cost combines one-off capital investment expenditures (CapEx) as well as annual operational expenditures (OpEx) over the 10 year period, both at EU level and at Member States level.

[96] See Gartner study on the "Sustainability and Efficiency of Visions for CISE" for more information, available on http://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance/index_en.htm

Assumed realisation potential of full CISE benefit	20%	40%	65%	50%	50%	50%
TCO – 10 years (M€)	60	75	106	86	86	86
EC costs	26	26	26	26	26	26
MS costs	34	49	80	60	60	60

Table 2 - Cost of the policy options (source: Gartner study)

7.4.2. *Cost at EU level versus costs at Member States level*

These costs can be further divided into costs likely to occur at EU level and those likely to occur at Member State level (which to a certain extent can be supported from the EMFF Regulation).

The distribution of cost over the 10 year budgeting period shows an initial investment needed at EU-level for developing an Information Exchange Model, common IT components and central support systems to CISE and a larger cost of the (gradual) connection of country systems to CISE.

The initial investments at EU-level are then followed by investments at the Member State level to offer and use new information services. The investments in the Member States are assumed to follow a bell-curve where few will invest early, and the peak of investments will be in year 5 and 6 of the budgeting period. This implies that the adoption of CISE at the Member State level is modelled to follow investment cycles in the Member States and not a centrally managed rollout plan.
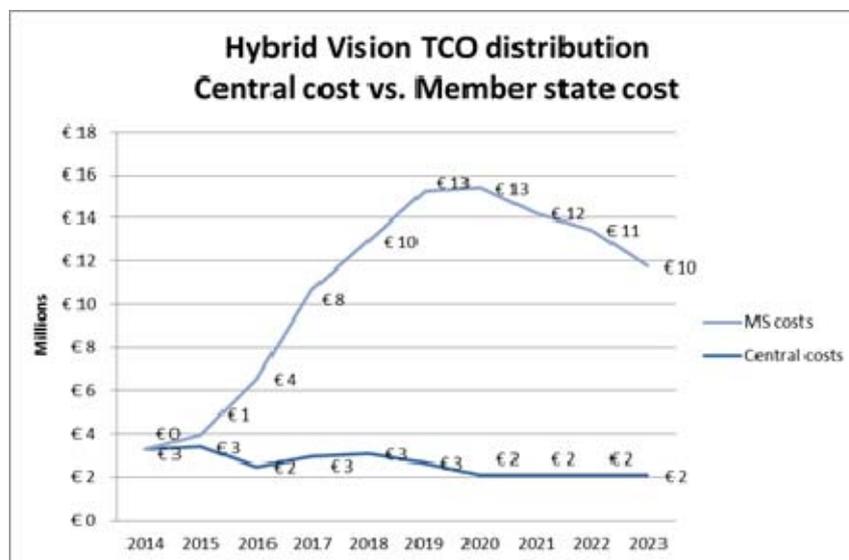

Figure 5 - Central cost versus Member States cost (source: Gartner study)

EU-level cost amounts to 26,1 M€ These include the set up and operation of the different components envisaged at central level, i.e. CISE governance, a common data model, a registry of services and authorities, a common collaborative platform, common monitoring

services, a reference implementation for the interface of systems, and increased exchanges of information between EU systems[97].

Note that the cost of implementing a reference implementation could be decreased by reusing existing solutions as explained in section 5.2.

Depending on the level of information exchange, the yearly Operating Expenditure (OpEx) for CISE is expected to amount between 85.000 € and 200.000 € per Member State, thus between about 2,5 M€ and 5,5 M€ for all CISE participants (reference year 2023).

It is understood that these are average figures. As results from the above, the burden may be higher for certain Member States than for others depending on Member States' existing situation and the resulting level of effort required to inter-connect through CISE.

8.   COMPARING THE OPTIONS

An overall assessment should now follow the qualitative and quantitative analysis.

		Short Term Effectiveness in achieving the objectives	Short Term Economic, social and environmental benefits*	Long Term Effectiveness in achieving the objectives	Long Term Economic, social and environmental benefits*	Cost
Option 1	Baseline scenario (reference)	0	0	0	0	0
Option 2	Communication	+++	+++	+++	+++	€
	Guidance document through a recommendation	+++	+++	+++	+++	€€
	Joint undertaking	++	+	+++	+++	€€€
Option 3	Amendments of sector legislation	++	+	++	++	€€
	Cross sector Regulation	+	+	+++	+++	€€
	Technical Regulation	++	++	++	++	€€

0: no change compared to baseline scenario; +: limited increase compared to baseline scenario; ++: moderate increase compared to the baseline scenario; +++: high increase compared to the baseline scenario

Table 3 - Comparison of the options

8.1.   Effectiveness in obtaining the objectives

The sub-option with the highest score would be to develop a guidance document through a recommendation since this option is the best suited in the short term to tackle the most

---

[97]   See Gartner study on the "Sustainability and Efficiency of Visions for CISE" for more information, available on http://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance/index_en.htm

fundamental problems, namely cultural barriers. It can however not obtain the highest score since it cannot tackle legal limitations and only to a certain extent technical limitations.

The adoption of a Communication also receives a relatively high score since it can constitute the necessary point of departure for the implementation roadmap process, by raising the awareness, by identifying the necessary steps needed towards implementation and by allowing all stakeholders to commonly develop the solutions that best fit their needs in a step by step approach.

Amendments of sector Regulation also receives a relatively high score since this option can address legal limitations and technical obstacles, but it does not receive a top score since these limitations may not be as many as expected. The same caveat applies to sub-option 3.3.

While a cross sector Regulation is considered ambitious in the short terms, in particular if taking into account the complexity and diversity of the current surveillance landscape and on-going actions, this option nevertheless has a high potential for the longer term future if in the meantime stakeholders can commonly develop the best fitting interoperability solutions. The legal complexity of such measure will nevertheless remain while in any case it won't cover the defence community.

Due to its inclusiveness, a Joint undertaking can be an effective means to implement the objectives, in particular in the medium term.

8.2. Benefits

The sub-option which receives the highest score is again the guidance document since this option constitutes an efficient tool to promote the removal of cultural barriers in the short term. This work can start more or less immediately and does not have to await the outcome of a legislative process.

The option of a Communication also receives a high score since it can establish the implementation roadmap process and political support for the process. As stated above, it can however not as such address limitations or implement any solution.

Amendments of sector legislations also receive a relatively high score since this option can achieve benefits, but those benefits will occur further downstream once the legislative process has been finalised. The same reasoning applies for the technical Regulation implementing EU standards for information exchange can lead to considerable benefits, but since the elaboration of those standards are expected to take some time; the benefits are further downstream.

The option that receives the lowest short term score in terms of benefits is the cross sector legislation. This is because the potential benefits are not expected until further downstream compared to the other two binding sub-options (due to the complexity of the matter) and will not be able to address the biggest hurdle, namely the cultural barriers. However, in the longer term, once stakeholders agreed on best fit legal, organisational, technical, semantic and policy aspects of interoperability solutions, it may be of high value added to establish those though a cross sectorial Regulation.

8.3. Cost

The non-binding options are the least costly options for Member States since they will not be required to take any measures to adhere to the common information sharing environment. At EU level cost will only occur for the development of recommended IT solutions and at Member States level they will only occur where solutions are implemented.

The most costly option for Member States and EU are the binding solutions for obvious reasons.

8.4. Conclusion

On the basis of the above, it seems that it will not be possible to achieve the defined objective though one policy option. Legally binding options can address legal and technical limitations but not for all seven sectoral functions and can further not capture cultural barriers. In particular, enhanced information exchanges between civilian and military authorities cannot be addressed through this option. Non-binding options are best suited to address cultural barriers (which seem to be the biggest hurdle to information exchange at least in the short terms) and can be considerably helpful in finding practical solutions which could involve all seven functions and thus enhance information exchange between civilian and military authorities. Those options do however fall short in addressing any legal limitations and technical barriers.

The best solution therefore seems to be to strive for a combination of several options in the short, medium and long term.

It seems that the best way to implement this work in the short term is to consider publishing a Communication which can provide an implementation roadmap and identify in concrete terms the work needed related to a corresponding timeframe.

Such action should be followed in the short-term with a guidance document to address first and foremost the cultural barriers and to establish best practices for information sharing. This document would also be useful to raise the awareness of the fundamental rights regarding the protection of personal data and ensure a common understanding of these issues within the field of maritime surveillance.

While in the short term a joint undertaking falls short in this perspective since the process for putting such a mechanism in place is relatively heavy, it may however have a lot of potential as a mid-term tool allowing for inclusive developments and research by stakeholders to find the best fitting interoperability solutions. Such an approach would however need further assessment as to its added value and suitability.

The sub-option on addressing legal and technical limitation through amendments of existing legislation over time seems to be the most proportionate and acceptable to stakeholders in order to avoid excessive EU action. This process can take place in conjunction with the ordinary revision process of the sector legislation when undesired limitations are identified, and also need to include a fundamental rights assessment in the accompanying impact assessment. Such an approach would also be relatively light compared to the option for a CISE Regulation and can therefore be smoother to implement and would not risk creating any inconsistencies with provisions in sector legislation. The developments of interoperability standards could be developed in accordance with the digital agenda of the EU.

A technical regulation may be a solution in the long term to deploy a standard in a coherent manner.

If needed, a cross sectorial Regulation may be envisaged on the long term.

The preferred option would therefore be a mix of options, 2.1, 2.2, possibly coupled with, 3.1, and 3.3 if such action is deemed necessary.

As a consequence, it is estimated that, compared to the baseline, this policy mix may realise 80 % of the full potential of the CISE project, while incurring 133 M€TCO realising 151 M€ cost savings, 460 M€ beneficial impact and may thus realise at least a progressive cumulated positive impact of 611 M€ over the first ten years during which CISE is being progressively set up.

Overall CISE is estimated to bring a beneficial impact within a range of 160 million € per year and 420 million € per year over the following ten years.

9. MONITORING AND EVALUATION

The European Commission will be monitoring the further development of the CISE project action plan through regular meetings with the Member State expert sub-group and the inter-service group on maritime surveillance as well as the Technical Advisory Group (TAG).

These groups will also be heavily involved in the drafting and the regular review of guidelines and handbooks which would be put in place for this purpose, in particular to address the gap between the demand and supply of maritime surveillance data identified in section 4.4.

Monitoring and evaluation indicators would be as follows:

General objectives	Indicators
To maximise the information exchange among maritime surveillance authorities in the EU.	Relative increase of data flows of information services between authorities
	Efficiency increase in maritime surveillance Reduction of duplication in data collection efforts
To increase the automatic treatment of data flows.	Relative increase of automated data flows.
Specific objectives	Indicators
To address all remaining legal limitations to information exchange among maritime surveillance sectors.	No of legal limitations
	Number of service level agreements between EU agencies and Member States
	No of legal acts referring explicitly to CISE
	Number of CISE projects financed by EMFF
To address cultural barriers for information exchange.	Number of co-operation projects and pilot projects under EMFF which fosters enhanced collaboration on information exchange issues
To put in place interoperability standards for	Number of legislative acts or agreements on

information exchange	common interoperability standards referring to CISE
	Number of service level agreements on technical standards

An evaluation of the implementation of the work ahead and of the regulatory measures will be carried out before the end of the period 2014-2020, with a view to assessing the need to define a new set of actions beyond that period. The evaluation of the implementation of the regulatory measures will continue at least for 2 years after they come into effect.

10. ANNEX 1: SUMMARY OF PUBLIC CONSULTATION

The public consultation summarised below was one element amongst many in terms of stakeholder consultations. As mentioned in the above, The Member States Experts subgroup and the Technical Advisory Group on CISE held numerous meetings to steer the political and technical process towards CISE, three large scale pilot projects each involving about fifty national authorities and EU level Agencies explored the need and the expected feasibility of CISE from the viewpoint of maritime surveillance practitioners and the Council supported the CISE process in numerous conclusions.

Further to that, a public consultation was conducted in the period 14 June – 14 September 2013 via the Commission's Interactive-Policy Making (IPM) tool. The consultation provided the possibility of EU citizens as well as non-EU citizens to express their view on the Common Information Sharing Environment (CISE) – as an input to the policy process of the European Commission. The below textbox provides an overview of the content of the questionnaire used in the consultation process.

Overview of questionnaire content

> **Introduction:** Providing respondents with information about the background of the consultation process as well as presenting basic information on CISE
>
> Questions about the **survey participant**: Gathering information on the respondent, affiliate administration/organisation, and maritime community
>
> Questions about **CISE themes**: Gathering information about views on current status of information sharing, including legal framework, cultural and technical barriers; as well as foreseen improvements with better information sharing
>
> Questions about **implementation options**: Gathering information about views on how best to implement CISE
>
> Questions about **CISE benefits**: Gathering information about views on the areas in which CISE can benefit, and by which magnitude
>
> Questions about **CISE services**: Gathering information about views on the development and supply of information services, standards, interoperability, public/private cooperation, and cost of provision.

The consultation process shows the attitudes of those who responded; and cannot necessarily be regarded as being representative of the entire population. As such, the consultation does not claim to provide a representative view of the general public's opinion of CISE; nor does it give a policy recommendation from the general public. These factors must be taken into account when analysing and using the results of the consultation process.

(a)   Questionnaire results

33 responses

The European Commission received a total of 33 responses to the public consultation on CISE. This must be regarded as a rather low number, and naturally limits the validity of the overview and analysis presented below. For the same reason, the analysis below has been kept on an aggregated level, i.e. including all types of respondents.

(b)   Respondents

Coverage of types of respondents

The responses to the public consultation have been somewhat uniformly distributed across (i) national administration; (ii) a combination of other types of organisations, including regional, European, international, non-governmental and professional organisations; and (iii) responses received from private companies. A lower number of responses have also been received from the scientific community and the general public.

Coverage of types of respondents

Number of respondents
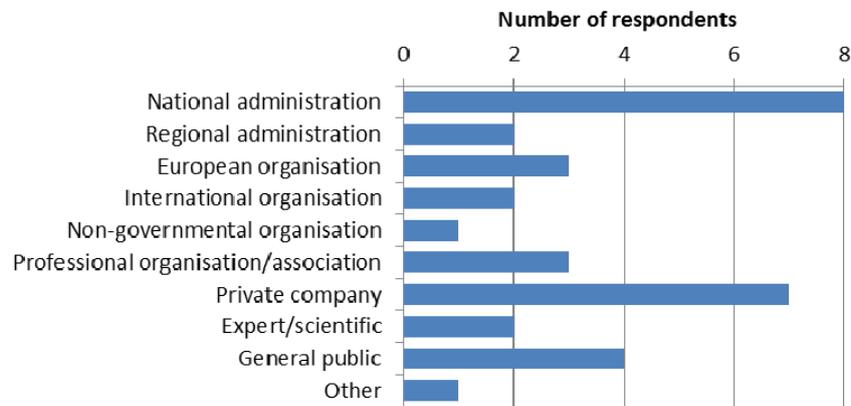
Source: Public consultation

Coverage of maritime functions

All maritime functions, except Customs, are represented in the survey. However, there is an overweight of responses from the maritime safety and security community, while only one response has been received from both the fisheries and the law enforcement community. Most of the private companies who responded listed themselves either as maritime surveillance systems and equipment manufacturers/suppliers or in the fisheries and aquaculture business.

Coverage of maritime functions

Number of respondents
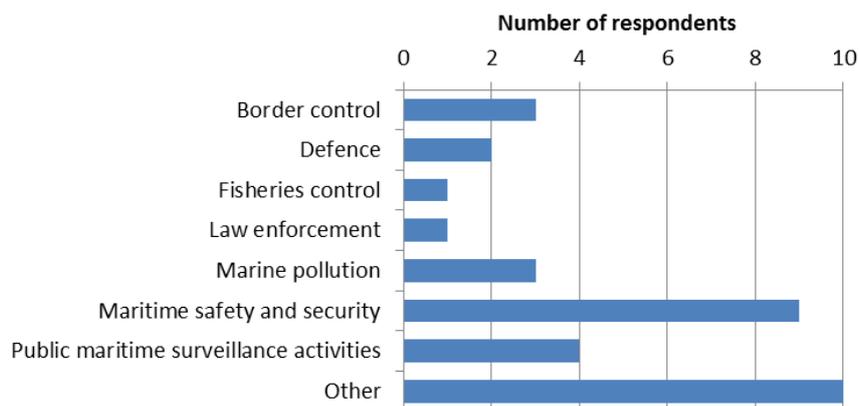
Source: Public consultation

While most of the responses have been received from national administrations, not all marine functions are covered. Indeed, the coverage is scattered across all the different types of respondents.

Types of respondents and maritime function coverage

Respondent	Safety and security	Border control	Defence	Fisheries control	Marine pollution	Law enforcement	Public maritime activities	Other	Total
National administration	2		1		2		3		**8**
Regional administration		2							**2**
European organisation	1							2	**3**
International organisation		1						1	**2**
Non-governmental organisation					1				**1**
Professional organisation/association	1							2	**3**
Private company	3							4	**7**
Expert/scientific			1			1			**2**
General public	2						1	1	**4**
Other				1					**1**
All	**9**	**3**	**2**	**1**	**3**	**1**	**4**	**10**	**33**

*Source: Public consultation*

(c)   Limitations to current level of information sharing

The first part of the questionnaire was designed to provide input about the current level of information sharing in maritime surveillance, as well as the limitations that currently exist as regards such sharing.

Current sharing between sectors and across borders is limited

Among all the respondents there was a clear sentiment that the public authorities, who are responsible for maritime surveillance activities, **do not** cooperate or share existing information between sectors and across borders in an optimal manner.

Agreement that public authorities do not cooperate or share information between sectors and across borders in an optimal way
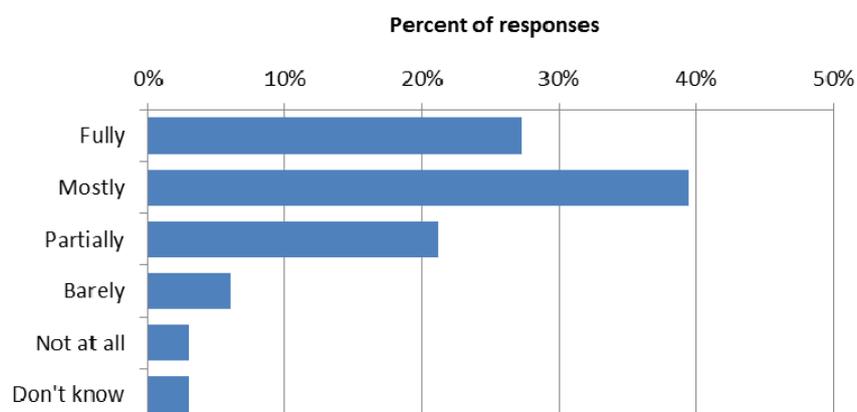

Source: Public consultation

Regulatory framework for information sharing

One of the reasons for the respondents' agreement on a sub-optimal level of information sharing between sectors and across borders is the underlying regulatory framework. In this regard, the degree to which the respondents agreed that the current regulatory framework at the international, EU, and Member State level limits such information sharing throughout the EU resembles, to some extent, the above picture.

Agreement that current international, EU, and Member State regulatory framework limits information sharing between sectors and across borders
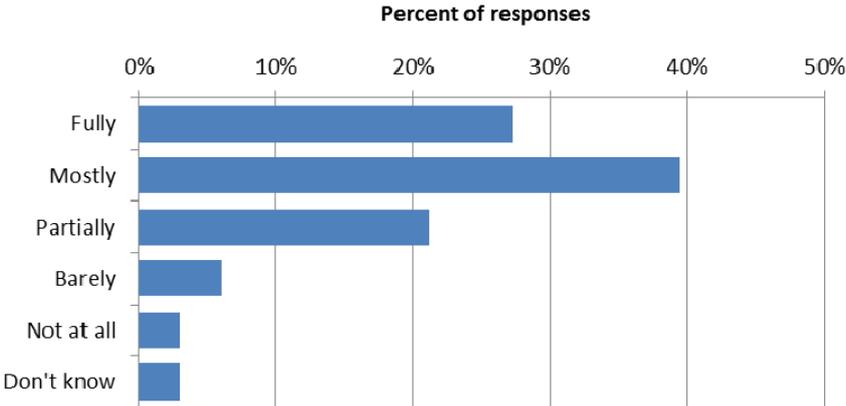

Source: Public consultation

Cultural barriers to information exchange

Historically, policies that govern maritime surveillance information sharing have typically been developed and organised with a particular maritime sector focus. From the questionnaire there is a strong indication that this sectorial approach have resulted in the built-up of cultural limitations to information exchange between the sectors.

Agreement that cultural barriers to cross-sectorial information exchange are the result of sectorial policies and organisation at both Member States and EU level.
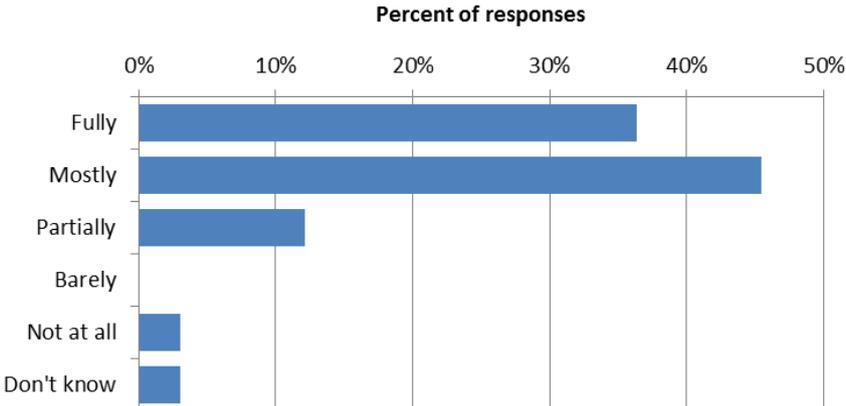
Source: Public consultation

Technical barriers to information exchange

There is less agreement that the above mentioned sectorial policy focus also have resulted in the built-up of technical barriers to exchanging maritime surveillance information. However, the sectorial policy focus is still very much seen as an important driver for today's existence of technical limitations, such as incompatibilities between systems, for information sharing.

Agreement that technical barriers to cross-sectorial information exchange are the result of sectorial policies and organisation at both Member States and EU level.

**Percent of responses**
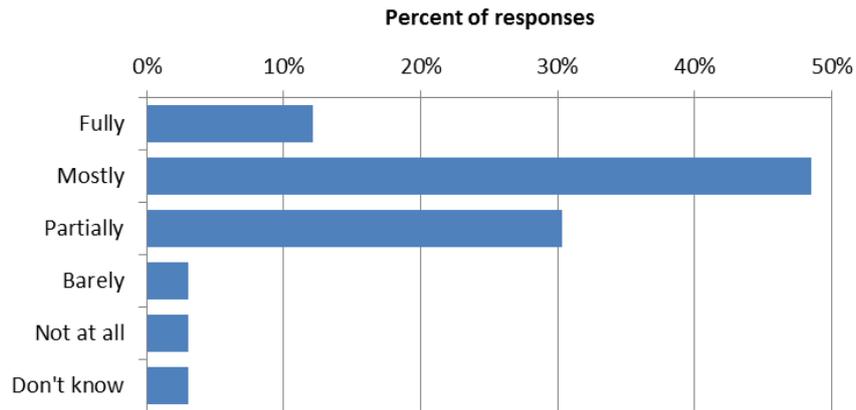
Source: Public consultation

Maritime situational awareness is not complete

One of the possible effects from limited sharing of maritime surveillance information is that relevant public authorities often do not have a complete understanding of the situation at sea, or "maritime situational awareness", which in turn may prevent them in taking the right and timely actions. This is also the view from the respondents where as many as 75% indicated their agreement (full or mostly).

Agreement that relevant public authorities do not have complete 'maritime situational awareness' often due to lack of information sharing between sectors.

Percent of responses
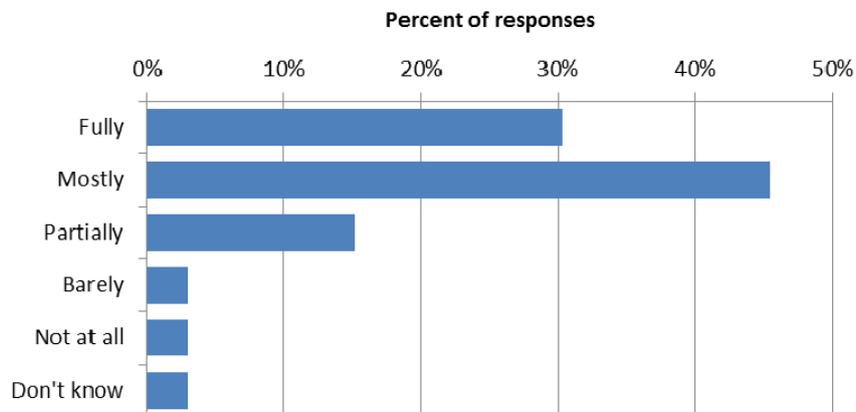
Source: Public consultation

Additional items highlighted by respondents

Concerning all of the items covered above, some 60% of the respondents have mentioned additional problems and/or limitations which they feel should be highlighted, based on their own experience. A categorisation and summary of these items is listed in.

Additional items highlighted by the respondents

Issue	Description
Data access restrictions	Member States have different rules regarding access to information. Sharing of information requires the development of common principles of information security and certification systems. Issues pertaining to privacy rights also need to be dealt

|	with
Cultural limitations	Authorities may not want to share their data due to confidentiality issues, lack of trust, competition.
Differing areas of competences	Authorities across Member States are not organized in the same way, and do not have the same tasks, rules, disciplines, etc. These differences can limit sharing and engagement in operations across borders.
Interoperability	Interoperability and harmonization of monitoring protocols for data sharing must be secured. Also, the interaction between final users, service suppliers and tools is currently fragmented across Member States and sectors; and has not been focused with a view to obtain a common and European-wide objective in the field.
Effective monitoring	Investment in human capital and technical resources and equipment is important to ensure a uniform and effective monitoring across the EU.
International cooperation	International cooperation on data sharing and common protocols should be promoted through the Neighbourhood Policy.
Collaboration between public authorities and private entities	Not well organised and could facilitate a potentially wider information sharing environment. Also, ship operators and shipping operations are perceived by some governmental agencies across the EU to be a part of the 'threat' not the 'solution'. As a result ship operators may therefore be unwilling to share data because the data invites unnecessary scrutiny and attention.

Source: Public consultation

One respondent also mentioned that there is a need for changing the attitude towards data sharing. For instance, as long as the data collector is an EU or Member State authority, and as the policy makers have agreed to build an EU Integrated Maritime Surveillance environment, then the data sharing **shall be enforced** on the collectors—and not requested on voluntary basis. From this perspective, a clear legal framework for IMO, IMS and CISE would be essential to ensure real progress.

(d)   Expectations from better information sharing

Improved information sharing could lead to benefits

There is a clear understanding among the respondents that current information sharing is limited, and, as a partial result, that relevant public authorities often lack full maritime situational awareness on which to base their action. In this light, there is also a very strong agreement that better information sharing between sectors and across borders could be expected to reduce the cost and improve the efficiency of maritime surveillance activities. Better information sharing is moreover expected to improve monitoring and surveillance, as well as lead to better safety and security at sea.

Agreement that improved information sharing between sectors and across borders could reduce cost and improve efficiency of maritime surveillance activities.

Percent of responses
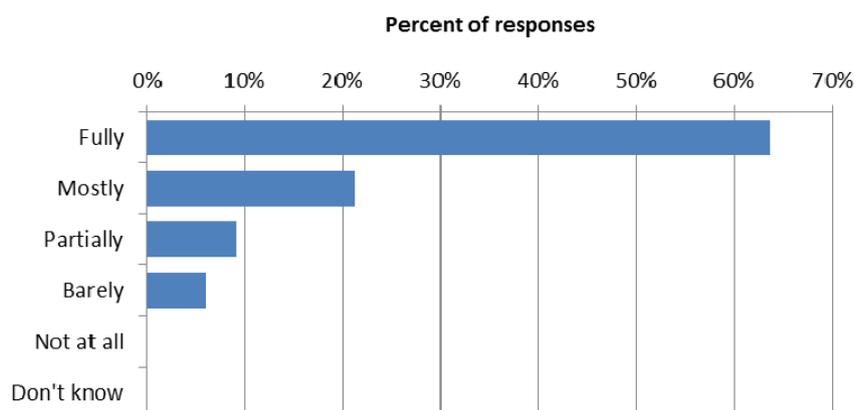
Source: Public consultation

Agreement that improved information sharing between sectors and across borders could improve monitoring, surveillance, safety and security at sea.

Percent of responses
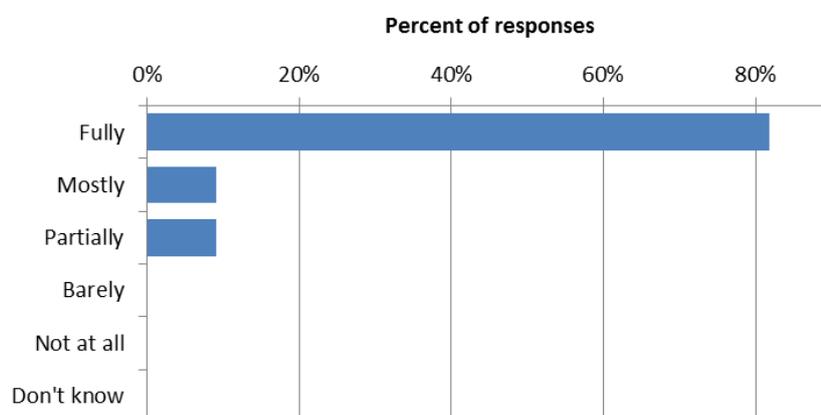
Source: Public consultation

(e)   Implementation of CISE

Action must be taken

Regarding the achievement of better information sharing in maritime surveillance almost all respondents disagree with the option of taking "no further action"; that is, things should involve as they are now.

*Agreement on "no further action" to implement CISE.*
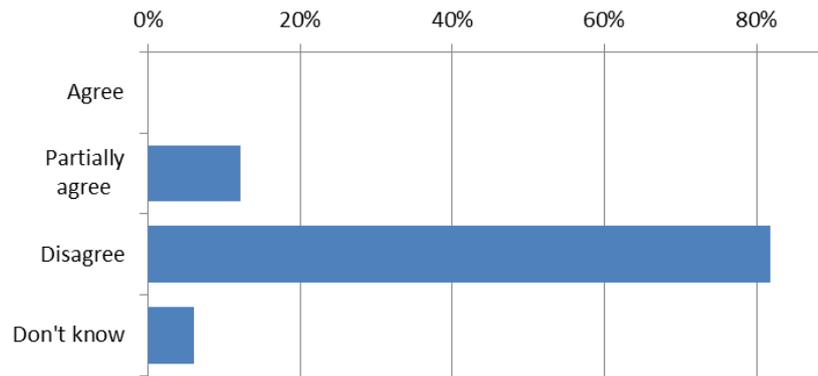
Source: Public consultation

CISE should be implemented through binding measures

Generally speaking, CISE could be implemented either though non-binding instruments, or through binding measures while also removing existing limitations (legal or other) where appropriate to ensure better information sharing. According to the responses to the questionnaire, the respondents favour the option of implementing CISE **via binding measures**. More specifically, 48% fully agree with using binding measures while an additional 39% are in partial agreement. For the non-binding option, on the other hand, only 21% are in full agreement, and 21% are in partial agreement. Moreover, almost 50% disagree that non-binding measures are the right option while only 9% disagree that binding measures are the right option.

Agreement on using non-binding or binding instruments for implementing CISE
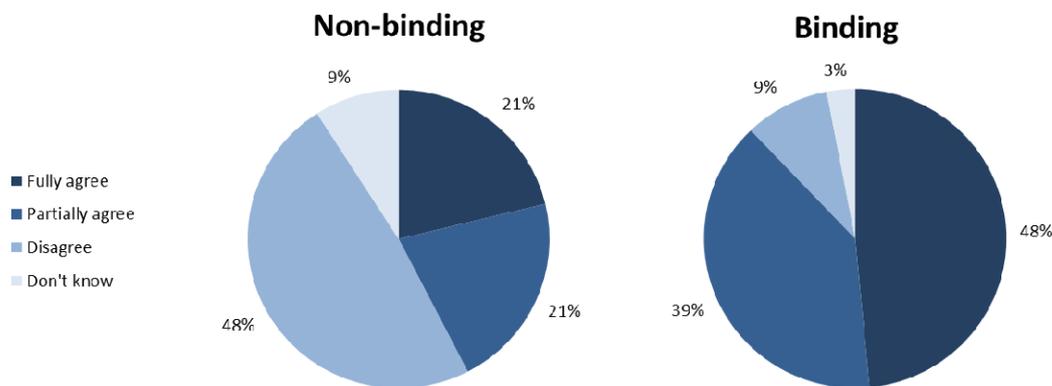
Source: Public consultation

CISE should be implemented step-wise

In connection with the replies to how CISE should be implemented several comments were raised by the respondents. While binding measures were the preferred option, several respondents were of the opinion that the implementation should be done in a step-wise manner; i.e. involving only a set of sectors and Member States with a willingness to collaborate at first, and then later expand with additional authorities. In this regard, it would be important to kick-off the process with a few "basic" or "minimum condition" binding instruments that would be supported financially by the EU to encourage cooperation. This

should allow for establishing a basic framework including common procedures, legal frameworks and technical conditions. As a general rule, however, the introduction of binding instruments should be shown to deliver "value for money" and be limited to areas where non-binding instruments prove not to be efficient.

Looking towards the future, and particular as regards the expected rise in maritime traffic over the coming 10-20 years, it was also mentioned that maritime and security measures should be optimised and include all countries around the European seas and straits, including non-Member States.

CISE should build on existing knowledge

Respondents also mentioned that the implementation of CISE should build on the knowledge, experience, and the demonstrated value added that are available from various pilot projects and initiatives, such as , EU NAVFOR (defence), EFCA MarSurv (fishery control), EUROSUR (border control). CISE should also take advantage of the awareness of technical innovations proposed by pilot projects like BluMassMed and MARSUNO and other initiatives launched in the context of the European research and development framework (FP7).

CISE should foster public/private partnerships

CISE should moreover focus on fostering the collaboration between public authorities, private suppliers and service providers, in order to implement and deploy an effective service based system for the wider information sharing in the maritime domain. Public-private collaboration in the implementation phase of new information sharing systems could be fostered by initiatives like the Pre Operational Validation (CLOSEYE) that benefits from FP 7 funding. In H2020 further activity in other parts of the EU should be allowed inviting administrations to get together and solicit industry involvement. New actors gaining access to the available information could lead to the development of new applications and services for the wider maritime community.

CISE should build on a clear message

A few respondents also highlighted a critique of the CISE process; i.e. mentioning that the learning from pilot projects and initiatives had not been leveraged to a satisfactory extent, and that the CISE initiative has been communicated in contradictory and confusion tones by the different DGs involved in the process. In this regard, the CISE TAG group should come up with a clear vision of what CISE is, how it should be implemented, and establish an agreement on how it should be supported and agreed upon at all political levels within the commission. In this process, the different agencies involved with maritime surveillance in the maritime domain should also take a more cooperative than competing role.

(f)   Benefits of implementing CISE

There is generally agreement among the respondents that CISE will deliver benefits in a number of different areas. The numbers of respondents who expect that CISE will **significantly** enhance the effectiveness of maritime surveillance activities as well as the response capabilities of operations are the most noteworthy, i.e. numbering nearly 80% and 70%, respectively. The following figure depicts the areas for which the respondents were

asked to provide their consideration as regards the magnitude of benefits. The areas have been sorted according to the areas with the highest expected magnitudes of benefits (combining significant and moderate benefits).

Expected magnitude of benefits of CISE in different areas

Percent of responses
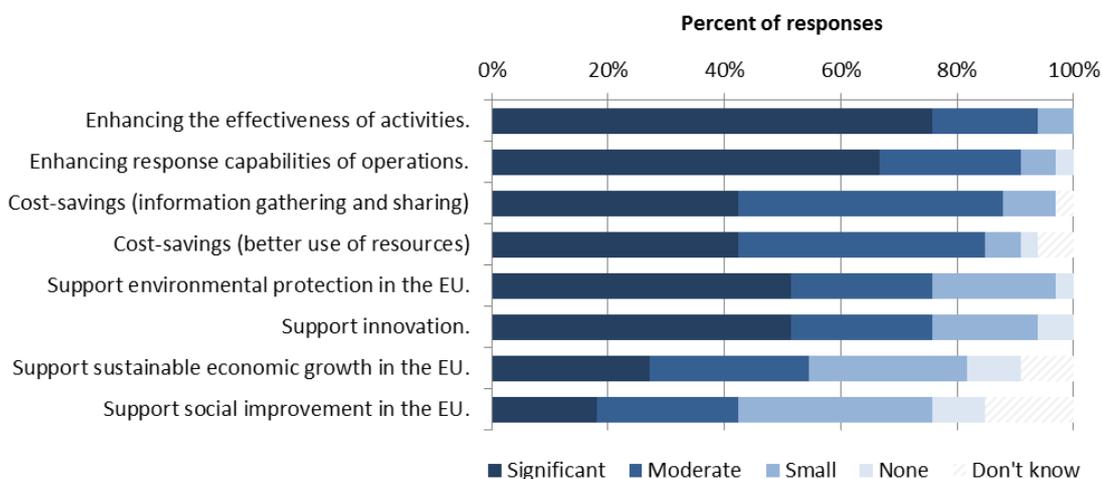
Source: Public consultation

CISE will bring large cost saving effects

After enhancing the effectiveness of maritime surveillance activities and response capabilities, the respondents also consider that CISE will bring large benefits in terms of cost savings. This includes cost savings from both information gathering, sharing and better use of resources.

CISE will support environmental protection and innovation

To a somewhat lesser extent than cost savings, albeit with a few more respondents expecting impacts with higher significance, the results show that 75% of the respondents expect benefits from CISE in terms of support of both environmental protection and innovation in the EU.

Sustainable economic growth and social improvement

About half of the respondents consider that CISE will have significant to moderate benefits in terms of supporting sustainable economic growth in the EU, while the corresponding figure is about 40% for the support of social improvement in the EU.

(g)   CISE services

CISE services could be developed through public private cooperation

Information sharing in the CISE will take place through a number of information services which can consist of predefined, regular, or ad hoc exchanges. These services can be subscribed to, or developed and published by, the relevant authorities. 60% of the respondents, however, think that such information exchange services also could be developed and published in cooperation between public and private bodies. Some 25% think that this should not be the case, while 15% are of no opinion about the matter.

Can information services be developed in co-operation between public and private bodies?

Percent of responses

| | 0% | 10% | 20% | 30% | 40% | 50% | 60% | 70% |

Yes

No

No opinion
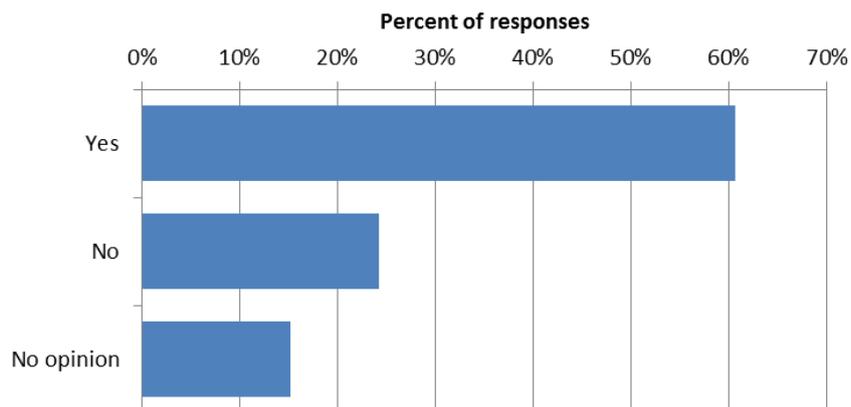
Source: Public consultation

Public-private cooperation would require common standards

Several respondents raised specific views on the public-private cooperative development of information services in CISE. For example, the success of public-private collaboration would depend on the development and application of common standards for conducting information exchange among all stakeholders, and which would also include appropriate confidentiality and security measures. Such requirements and standards would nonetheless also need to take the technical capabilities and standards of industry into account.

Private entities are involved in other areas

In initiatives similar to CISE, such as EUROSUR and the Single Window reporting, private entities are to a certain extent also involved; i.e. shipping agents, ships and their managing companies, etc. This could serve as a point of reference for CISE.

Private entities could contribute to rich development environment

Opening the development of information services to also include private entities based on a common standards approach could also ensure competition in the market for developing and supporting information services. In turn, this could create a vigorous services development environment, not unlike the one which has been established in the mobile communications industry, and thus bring a long range of additional benefits to the different maritime stakeholders through the more effective use of available information resources. In the longer run, CISE could grow to become a platform for private entities to develop and offer new smart surveillance tools.

Relevance of including private entities

The following table summarises the different perspectives that respondents have on the relevance of involving private entities in the development of information services

Views on the relevance of involving private entities in the development of information services

Relevance area	Description
Private industry is an important player in the maritime domain	Private industry plays essential role in maritime domain. Ships are private assets operated under private agreements; off-shore activities are privately driven, including many safety and security requirements under industry responsibility. Leaving industry outside of a cooperative data-sharing environment could therefore be a strategic mistake
Local interest and coverage of services	The involvement of private (local) stakeholders can secure a high degree of local awareness and participation. Especially in strait areas this can promote better security readiness in case of maritime accidents.
Leveraging knowledge and technical knowhow	The participation of the private sector can provide both the knowledge and the technological knowhow that is needed to develop useful and effective information sharing services in CISE across a number of areas.
Innovation driver	Including private entities can provide different perspectives, mutualisation and cost effectiveness in the development of services, and thus drive innovation. It can also contribute by including relevant research programmes.
Intellectual property issues	There may be a need for protecting industrial intellectual property.
Incentive and security issues	As private entities are driven by commercial interests and financial gain this could create a potential incentive conflict with public stakeholders driven by improving surveillance effectiveness and efficiency. Commercial interests may also conflict with the protection and/or sharing of information obtained under CISE, which could be an issue.
Cultural issues	Authorities may expect that communication is one-way; i.e. from industry to authorities, which could affect collaboration and involvement of private entities. This is for instance seen in supply chain security where certain authorities want to separate channels/views/systems from logistics industries as a condition for cooperation.

Source: Public consultation

Feasibility of integrating existing systems into CISE

There is generally agreement among the respondents that it not only would be feasible to integrate existing or developing products, technologies, systems and services for surveillance and intelligent data sharing at sea into the CISE by 2020; it would also be necessary. The following table provides a summary of respondents' perspectives in this regard.

Summary of perspectives on the feasibility of integrating existing and developing products, services, systems, and technologies into the CISE by 2020.

| Is it feasible?	Summary of perspectives
Yes	It is consistently feasible, although it depends on the specific product, technology, system, service maturity and impact on existing platforms. Some of them have high readiness and imply relatively low effort to be integrated.
	Some technologies have already reached the level of sufficient maturity to be used in the CISE within 2020. However specific improvements in the technical field could provide a significant improvement in the overall quality of CISE, and at the same time the development of CISE might stimulate the appeal for a standardisation of maritime technology across Member States, thus extending the use of proven existing systems and best practices.
	Full interoperability and reliability of existing maritime surveillance technologies

	within the wider framework of information sharing between actors in the EU should be pursued. Efforts should also focus on creating the right, modular, easily accessible business ecosystem for information services.
	Using an open architecture could ease the process. And knowhow and experiences from the collaboration between public bodies and private companies in other areas should be exploited.
Yes, but	With a positive political will the integration is highly likely to be possible. However, national and sectoral commitment is also essential. Hence, a political consensus and agreement must be reached at the EU level, including all involved DGs and their agencies. The integration would moreover require financial support to relevant EU institutions/agencies.
	Some technologies are already ready to be used in CISE. Other ones will be ready in horizon 2020. However, the necessary technological conditions will not be in place in all cases, and it is doubtful whether it will be possible to interlink systems across all EU members by 2020. The point is for the EU to find a suitable normalisation of the products, to help Members States share maritime information in a proper way. This will make it easier to reach a good level of interoperability between the existing maritime surveillance systems and services. Integration could also be widened by using a step-wise approach, i.e. using a roadmap for entry with feedback loops to amend gaps and shortcomings.
	Regional integration could be achieved faster.
No	The timeframe is too short

Source: Public consultation

A common data model for exchange should be based on standards

In order to improve interoperability, the CISE will make use of a common data model for data exchanges between systems and sectors. More than half (52%) of the respondents agree that such a data model standard should be endorsed by a recognised standards body. Only 9% did not see such an endorsement as necessary, while 36% had no opinion of the matter.

Should the standards for CISE's common data model be endorsed by a recognised standards body?
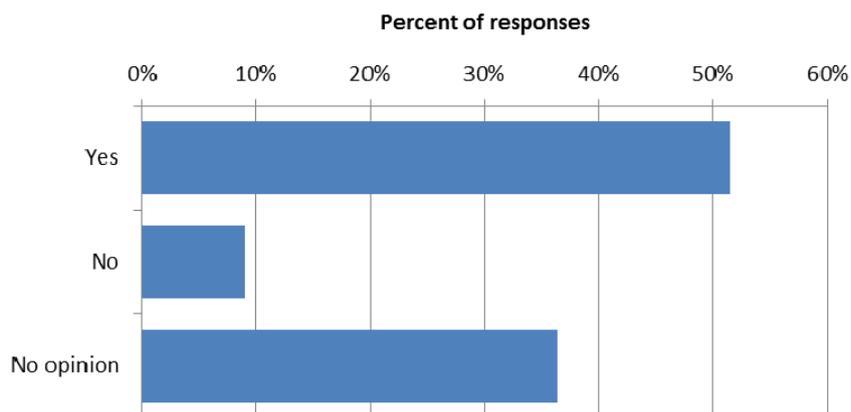
Source: Public consultation

The table below summarises additional remarks made by the respondents.

Summary of perspectives on whether the common data model standards should be endorsed by recognised standards body

Endorsement	Summary of perspectives
Yes	Technical commonality would seem to be a vital aspect of any EU wide system and therefore clear and precise technical standards would need to be identified and implemented. Also, common data formats and data models are essential for the effective sharing and correlation of data. They moreover facilitate access to the data, allow the creation of consistent procedures for data acquisition, reduce response time, and make it easier to include more participants.
	Suggested standards bodies include: ISO, CEN, EU-COM
	Remarks were also made that the standards body should be European. Also, the creation of an "EU Advisory Board" could coordinate and facilitate the process.
Yes, but	Interoperability could benefit from an official standardisation process although this could introduce a considerable delay, hindering the 2020 target. On this basis a two-step approach could be used. First, design good foundations for the reference data model and pushing to extensively adopt it. Second, once the data model is consolidated, start the formal standardisation process.
	A different perspective is that CISE should not define one common model, but a library of models based on existing standards and let the communities to decide which one fits best their existing set-up. Interoperability is well defined and standardised already and technically there are solutions to fit any existing architectures.
No	Technology is running ahead of standards bodies which are slow to follow. The best standards are therefore de facto.
	No need for standards. Just an open standard architecture.
	The development of common data model will involve a large number of institutions and businesses who will approve of the model.

Source: Public consultation

Most respondents are already exchanging data

Some 58% of the respondents are currently already exchanging data with other organisations that is relevant for maritime surveillance. 15% are not engaged in such activities. The remaining 27% have not indicated if they are currently sharing or not.

Do you already exchanging data with other organisations that is relevant for maritime surveillance?
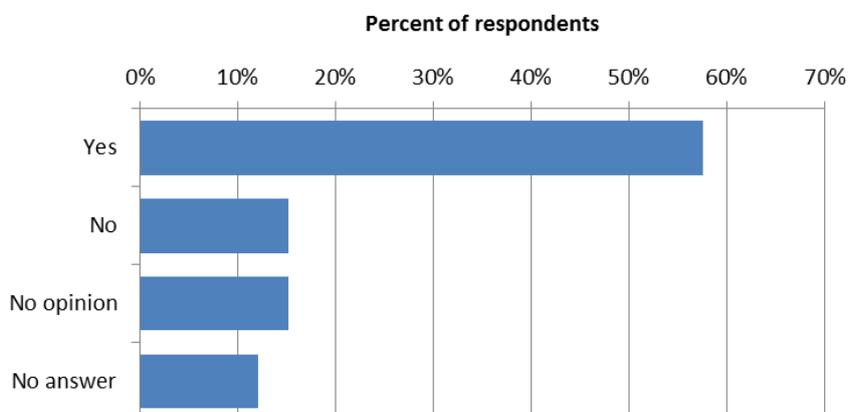

Source: Public consultation

In connection with the above there is no clear cut picture whether the respondents use specific standards in their information exchange. Some base their data exchange on standards; others only use standards for some exchanges but not all; while others again do not use standards. Also, standards have not been developed or applied in all areas of the respondents' information exchange, which naturally impede its usage. In some cases, standards are required for information cases, while in others they are used on a voluntary basis.

CISE would benefit from agreed technology and open source

Most of the respondents (52%) think that CISE would benefit from agreeing on a technology stack and from using an open source software development platform. The remaining 48% of the respondents have either not answered the question or given no opinion. As such no respondents disagree that an agreed technology stack and an open source platform would be beneficial.

Would CISE benefit from an agreed technology stack and an open source software development platform?

Percent of respondents
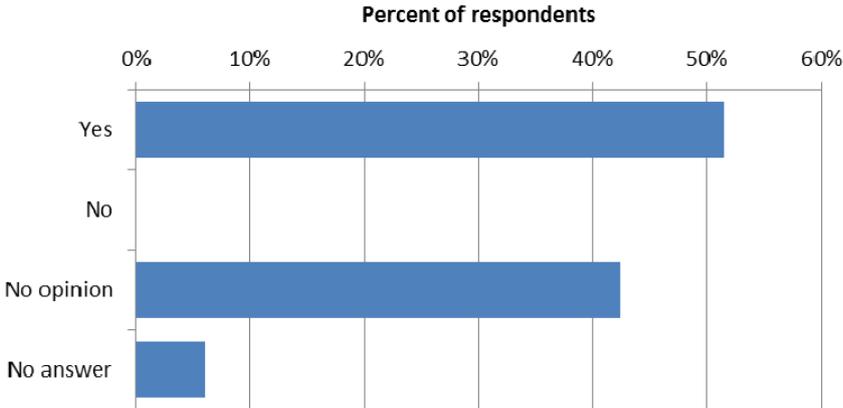
Source: Public consultation

Even if there is broad agreement on the benefits of agreeing on a technology stack and using an open source platform for CISE, there are only scattered views on what such a stack should include, and why. The main view appears to be to base CISE on a service oriented architecture based on an existing library of standards in order to enable the possibility for continuous and cost-effective updates and maintenance.

Cost of supplying information services

Respondents were also asked to provide information on their expected cost for making data available through CISE, and if they are in a position to cover these cost.

Several of the private organisations indicated that the question was either not applicable to them, or too complex to answer. Views from national administrations differed. For some, the cost would amount to between EUR 1-2 million and thus impede the administrations from covering the cost. Others could not say and referred to the issue being a matter of political decision. A European organisation put the cost much lower, i.e. between EUR 100,000-200,000, and thus within budgetary limits.

Several respondents mentioned that the cost would depend on the chosen degree of interoperability and available APIs for CISE. For some respondents, budgets could probably still cover the cost, while for others it is not possible to say at this point.

Return from CISE is expected to be higher than its cost

Some 30% of the respondents expect return from CISE to be higher than its cost. This is significantly higher to the 6% who do not expect the return to be higher. However, with 45% of the respondents having given no answer to the question, and 6% being of no opinion on the matter, it appears that there is a great deal of uncertainty about the capability of CISE to deliver returns that are higher than its cost.

Do you expect the return from CISE to be higher than its cost?
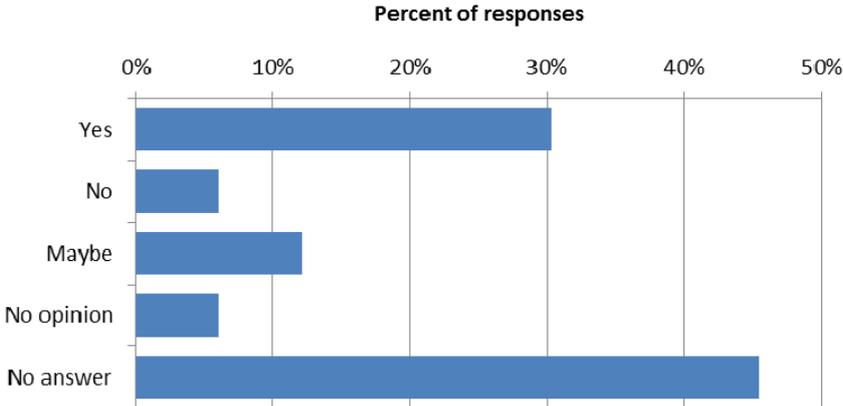
Source: Public consultation

(h) Concluding remarks

The low number of responses to the public consultation makes it difficult to make sound analysis on the provided answers. However, that being said, it appears that there is wide agreement that the EU economy and society will benefit from CISE, and that the platform can enable new innovative solutions for a more efficient and cost-effective use of available maritime surveillance information solutions.

Current situation is inadequate

There is broad agreement that the public authorities involved with maritime surveillance do not cooperate or share existing information between sectors and across borders in an optimal manner. This is mostly perceived as being due the underlying legal framework and a historical sectorial focus; which in turn prevents public authorities in gaining an adequate maritime situational awareness in support of their activities. Technical limitations to information sharing are seen as less of an issue.

CISE will improve maritime surveillance

The large majority of respondents agree that CISE will improve maritime surveillance; particularly with respect to enhancing the effectiveness of surveillance and the response capabilities of operations. Cost savings in terms of information gathering and use of resources are also highlighted as outcomes of CISE.

CISE should be implemented through binding measures

Almost all respondents disagree that no further action should be taken in the area of improving information sharing. Moreover, a majority of respondents agree that CISE should

be implemented using binding measures. The development of CISE services would furthermore benefit from cooperation between public and private entities. There could however be a need for establishing a clearer view of CISE.

CISE could benefit from standards and open source

CISE could benefit from building upon existing standards, an agreed technology stack, and an open source platform. It would furthermore be preferable if the implementation of CISE would use a step-wise approach, perhaps through the support from a well-defined roadmap.

11. ANNEX 2: SUMMARY OF THE MEMBER STATES SURVEY

1.1 Cost of current maritime surveillance

Introduction

The results of the MS survey regarding cost of maritime surveillance are presented below. Since the figures provided by the Member States are very incomplete, it is difficult to draw general conclusions and to get a good estimate of the surveillance cost baseline.

Results

The results are presented in the tables below:

Table 11-1 Operation and investment cost

	Operating costs 2012 (MEUR)	Forecast (2-3 years)	Investment cost (MEUR)	Forecast (2-3 years)
Belgium (MRCC/VTMIS)	3,6	-	-	-
Belgium (Defense)	1,0	1	-	30 MEUR
Finland (Fisheries control)	0,8	1	1,5	2
Finland (pollution)	4,8	2	3,2	3++
Finland (customs)	-	0	-	-
Finland (border control) *	61,7	2	36,45	1
Finland (defense)	2,0	-	10	2
France	-	-	-	-
Germany	-	-	-	-
Greece (defense)	111,7	-	-	-
Ireland	20,0	-	-	-
Italy	2272,6	0	1090,1	0
Latvia (defense)	4,1	1	6,75	0
Lithuania (defense + maritime safety)	1,3	0	0,43	2
Netherlands	-	-	-	-
Norway	-	-	-	-
Poland	-	2	-	2
Spain	190,0	0,5	50	1
United Kingdom	-	-	-	-

* Average Finnish border control (2008-2012) are 17.6 MEUR investment and 29.96 MEUR operation

Forecast code: 0: reduction, 1: stable, 2: increase up to 20%, 3: increase above 20%.

Table 11-2: Number of people employed (annual full time equivalents)

	Total	Administration	Forecast (2-3 years)	Operational	Forecast (2-3 years)
Belgium (MRCC/VTMIS)	150	20	0	130	1
Belgium (Defense)	10	3	2	7	1
Finland (Fisheries control)	22	12	1	10	1
Finland (pollution)	14	8	-	6	-
Finland (customs)	-	-	1	3	2
Finland (border control)	685	137	0	548	0
Finland (defense)	212	12	1	200	1
France	-	-	-	-	-
Germany	-	-	-	-	-
Greece (coast guard)	5960	4430	1	1530	1
Greece (defense)	5203	1039	1	4164	1
Ireland	2000	-	-	-	-
Italy	51000	6000	0	45000	0
Latvia (defense)	230	23	1	207	1
Lithuania (defense + maritime safety)	131	41	0	90	2
Netherlands	-	-	-	-	-
Norway	97	7	-	90	-
Poland	-	-	1	-	1
Spain	13400	400	0,5	13000	0,5
United Kingdom	-	-	-	-	-

Forecast code: 0: reduction, 1: stable, 2: increase up to 20%, 3: increase above 20%.

1.2 Limitations to information sharing

Introduction

In the second part of the survey Member States were asked to provide answers about the extent of limitations to information sharing; including the extent to which the limitations arise from (1) technical limitations; (2) cultural and/or administrative differences; and (3) legal limitations.

A total of 13 Member States provided answers to experienced limitations. However, some only provided answers for certain user communities. In general, the received data should be interpreted carefully as

- the low and high scores could be expressions of low need for exchange between user communities;

- limitations are mostly expressions of "targeted actions";

- less focus is put on routine exchange and thus the unknown.

Results

On average across all user communities there are about 25% cases of occasional and often experienced limitations to data access in the responding Member States. There are, however, most cases registered within the General Law Enforcement, Defence, Border Control and Maritime Safety user communities. As regards limitations seen from the providing part, only few communities experience limitations to obtaining access from the Maritime Safety and

Marine Pollution communities, while data access from General Law Enforcement, Defence, and particularly customs are experienced as more restrictive and limited. Overall,

- limitations are larger between Member States compared to within Member States;

- but experience of limitations also differs depending on whether the user community is receiving or providing information.

In terms of the types and overall significance of limitations to data sharing with respect to the different user communities, the results are the following:

Figure 11-1: Overall significance of barriers within MS
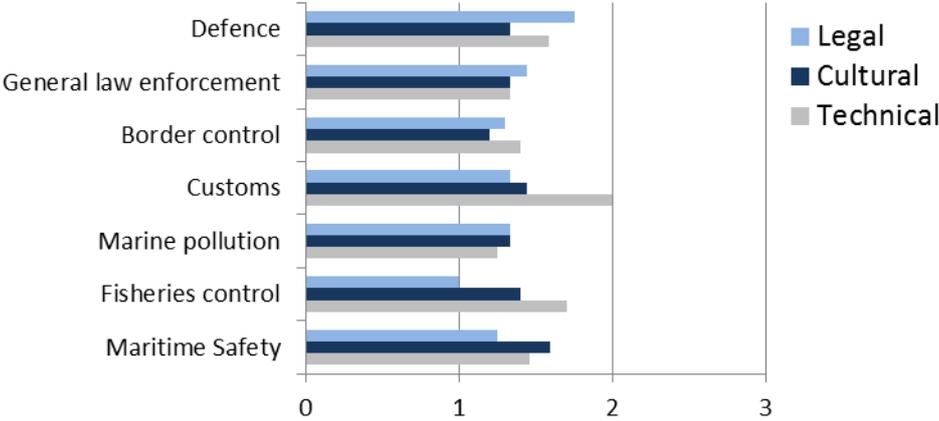
Explanation: 0:none, 1:minor, 2:moderate, 3:significant.

Figure 11-2: Overall significance of barriers across MS
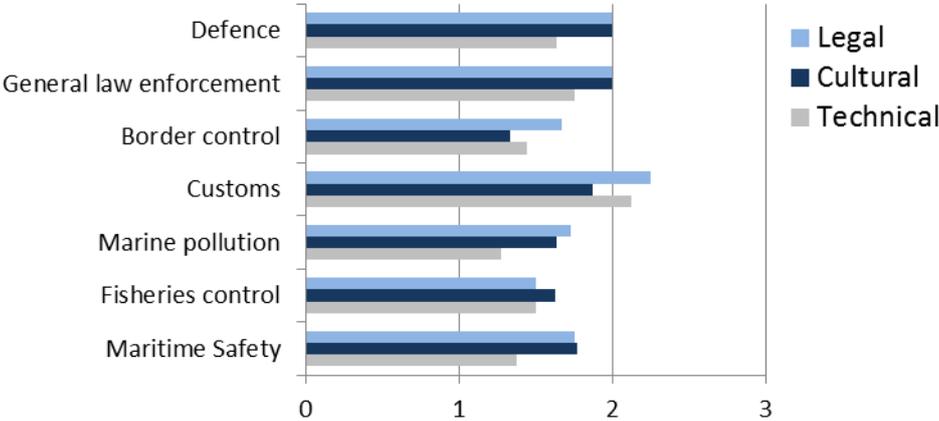
Explanation: 0:none, 1:minor, 2:moderate, 3:significant.

1.3   Benefits from CISE

Introduction

The third part of the survey addressed both potentials regarding surveillance tasks, i.e. routine tasks, targeted operations and response operations, as well as the types of benefits that Member States would regard as most likely to be realised.

Results

In terms of surveillance tasks, Member States generally see moderate to significant benefits across the board, albeit with targeted operations showing the largest potential

Figure 11-3: Overall benefits per Member State
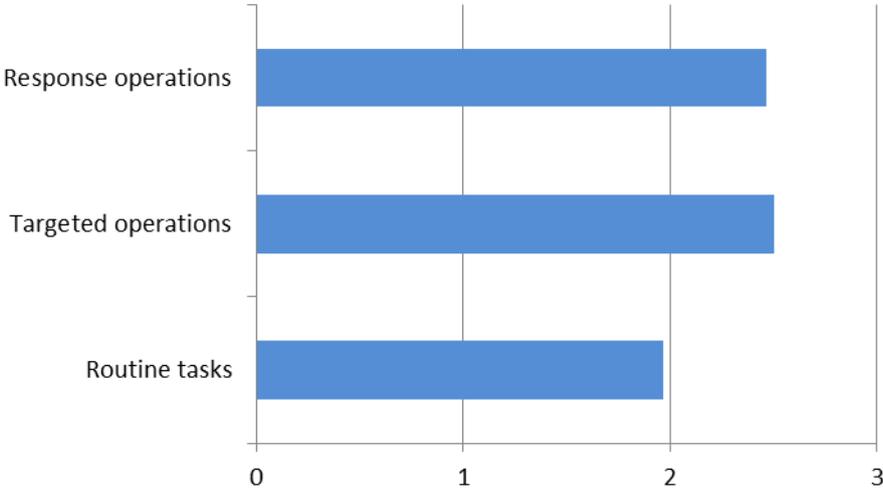
Explanation: 0:none, 1: small, 2:moderate, 3: significant.

Figure 11-4: Overall benefits per Member States (number of answers)
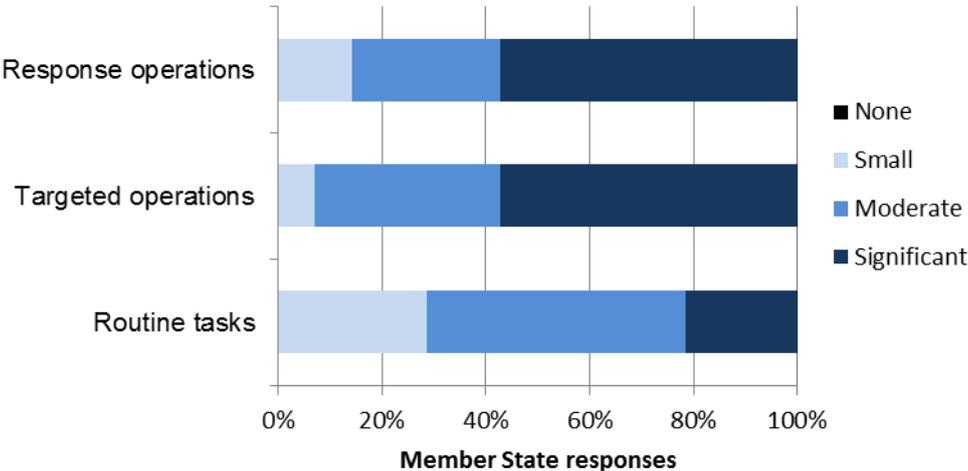
1.4   Impacts

Introduction

Examples of economic impacts:

- support a safe and competitive maritime space;
- reduction in foregone tax/import duties;
- fairer competition.

Examples of social impacts:

- improved sense of security:

- reduction in organised crime, particularly from better control of weapons and drugs smuggling

- examples of environmental impacts:

- better preventive monitoring

- faster response to environmental damages/disasters

Results

The results are presented in the figures below:

Figure 11-5: Overall impacts per Member State
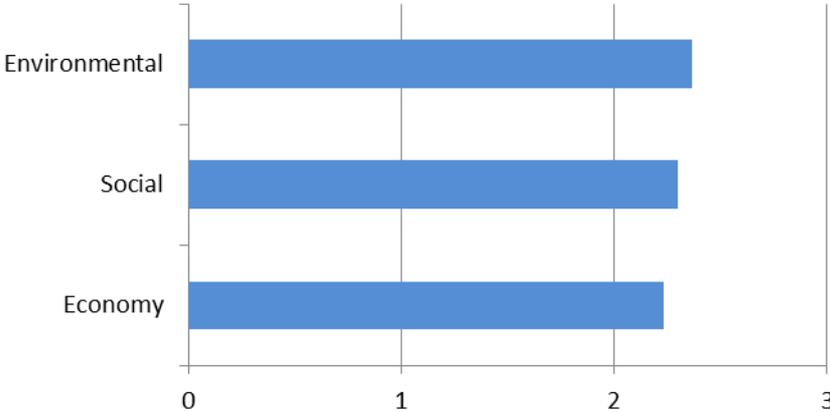
Explanation: 0:none, 1: small, 2:moderate, 3: significant.

Figure 11-6: Overall impacts per Member State (number of answers)
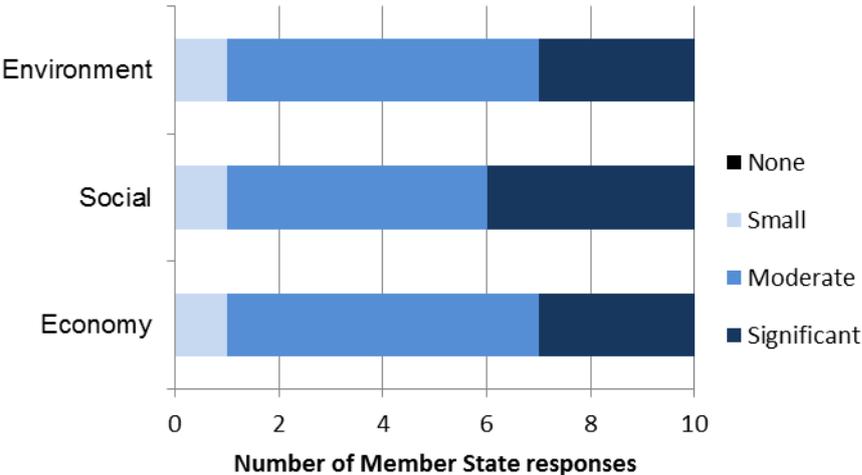
12.   ANNEX 3: MARITIME SURVEILLANCE AUTHORITIES IN EU MEMBER STATES

BELGIUM

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
The Belgian Coastguard (1) MRCC Ostend (safety)(2) Maritime Security Center Belgium MSC(B)(3) Shipping Assistance Division (of the Agency for Maritime Services & Coast) responsible for VTS and SAR	Department of Agriculture and Fisheries(4) Ministry of Defence (MOD) Federal Public Service interior (Martime& river Police) Federal Public Service Finance(Customs)	Federal public service Health Food chain safety and environment. Management (MUMM) (5) MOD - Belgian Navy (6)	Federal Public Service Finance (Customs)	Federal Public Service interior (Martime & river Police) Federal Public Service Finance (Customs)	Federal Public Service interior (Belgian police) (7)	MoD - Ministry of Defence- (Belgian Navy)

(1)The Belgian Coastguard is responsible for the cooperation between the partners authorised for the Belgian part of the North Sea, 17 governmental institutions (both regional and federal).

(2) MRCC is a division of shipping Assistance Division which is part of the internal independent Agency for Maritime Services and Coast, an agency of the Flemish Authorities. The MRCC together with the MSC(B) form the Belgian coastguard center.

(3) MSC (B) together with the MRCC form the Belgian coastguard center. 3 departments work close together: Ministry of defence (MOD), Federal Public Service interior (Martime & River Police) , Federal Public Service Finance (Customs).

(4) An agency of the Flemish Authorities.

(5) The Management Unit of the North Sea Mathematical Models (a federal scientific establishment that comes under the Federal Science Policy). Main role of MUMM in this context is to provide scientific advice on all environmental issues.

(6) In case of severe pollution incident (activation of the North Sea contingency Plan) the Belgian Navy is the overall coordinator of the activated Pollution Response Cel.

(7) Law enforcement in Belgium is conducted by an integrated police service structured on the federal and local levels.

BULGARIA

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Ministry of Transport, Information Technology and Communications - Bulgarian Maritime Administration/ Ministry of Interior/ Ministry of Defence	National Agency of Fisheries and Aquaculture	Ministry of Transport, Information Technology and Communications - Bulgarian Maritime Administration/ Ministry of Interior	Ministry of Finance - Customs Agency	Ministry of Interior - Police/ Ministry of Defence - Bulgarian Navy	Ministry of Interior - Police/ Ministry of Defence - Navy	MoD - Bulgarian Navy

CROATIA

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence

CYPRUS

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Dpt. Of Merchant Shipping/ Marine Police/ Cyprus Ports Authority/ Civil Defence Service/ Ministry of Defence	Dpt. For Fisheries and Marine Research	Dpt. For Fisheries and Marine Research/ Dpt. Of Merchant Shipping	Dpt. Of Customs	Marine Police	Ministry of Justice & Public Order (Police)/ Dpt. of Merchant Shipping	Cypriot National Guard - Naval command

DENMARK

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Danish Maritime Authority/ MoD- Royal Danish Navy- Admiral Danish Fleet/ Danish Coastal Authority/ Ministry of Transport and Energy (ports)/ Emergency Response Committee(1)	Ministry of Food, Agricultureand Fisheries - the Danish Directorate of Fisheries/ Ministry of Defense	Danish Environmental Protection Agency (law)/ The Admiral Danish Fleet is responsible forthe maritime/ anti-pollution response/ Local municipalities when pollution reaches the shore	Ministry of Justice/ Customs Authority/ Admiral Danish Fleet and Naval Home Guard may be used to embark Customs officers at sea	Ministry of Refugees, Immigration and Integration Affairs/ Local Police districts/ Admiral Danish Fleet will provide maritime surveillance and enforce national sovereignty at sea	Ministry of Justice and local police districts/ Danish Authority for Enterprise and Construction (rules on dual use products)/ Admiral Danish Fleet/ Customs Authority and Danish Maritime Authority may provide the legal basis for law enforcement	MoD - Royal Danish Navy

(1) The Emergency Response Committee consists of the Danish Energy Authority (chair), the police in Esbjerg, the Admiral Danish Fleet, the Danish Environmental Protection Agency and the Danish Maritime Authority. It supervises all measures taken by the op

ESTONIA

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Maritime Administration/ Governmental crisis commission/ Ministry of Interior/ Maritime Rescue and Coordination Centre	-Ministry of Environment - Environmental Inspectorate/ Estonian Border Guard -Ministry of Agriculture	-Ministry of Interior -Border Guard	Estonian Tax and Customs Board	Border Guard	Police	MoD - Estonian Navy

FINLAND

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Policy: Ministry of Transport and communications, Ministry of the Interior (SAR), *Operational aspects:* Finnish Maritime Administration (1)/ The Border Guard of Finland (at sea)(2), Rescue departments (harbours), the Finnish Environment Institure, Finnish Navy (3)	*Policy matters*: Ministry of Agriculture and Forestry-Department of Fisheries and Game *Operational aspects/controlling*: Regional Centers for Economic Development, Transport and Environment (ELY), police, Finnish border guard, the Finnish customs	*Policy*: Ministry of the Environment *Operational aspects:* Finnish Environmental Institute (in cooperation with the Navy, The Border Guard of Finland, Finstaship (=state-owned shipping company), and the local rescue authorities) Pollution prevention: Ministry of the Environment, Ministry of Transport and Communication, Ministry of Agriculture and Forestry	*Policy:* ministry of finance *Operational aspects:* Customs Authorities (=The Finnish Customs)/ The Border Guard of Finland (immigration)	*Policy*: Ministry of the Interior *Operational aspects:* Border Guard (with coast guard districts) *Policy related to maritime surveillance:* Ministry of Defence *Operational aspects:* Navy	Police/ The Border Guard of Finland/ Finnish Customs	*Policy:* MoD *Operational:* Navy with Border Guard (Coast Guard) in the times of war

(1)the ministry of social affairs and health is responsible for the working conditions onboard the ships and respective inspections carried out by industrial safety administration

(2) Border Guard is responsible of SAR and SSAS-alarms, the Finnish Navy conducts maritime SAR operations with and under the Border Guard

(3) in case of military crisis or war, Finnish Navy protects maritime traffic and transport with Border Guard (CG)

FRANCE

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
-Ministry of Transport (Admin. Of Mar. Affairs) -Ministry of Justice -Ministry of budget (Customs) -Ministry of Interior (home office-civil protection, gendarmerie) - MoD (navy - gendarmerie maritime)	- Ministry of Transport (Admin. of Mar. Affairs) -MoD (Navy - gendarmerie maritime) -Ministry of Budget (Customs) - Ministry of Interior (gendarmerie)	-Ministry of Transport (Admin. Of Mar. Affairs) -Ministry of Justice -Ministry of budget (Customs) -Ministry of Interior (home office-civil protection) - MoD (navy - gendarmerie maritime)	Ministry of Budget (customs)	-Ministry of budget (Customs) -Ministry of Interior (home office-civil protection) - MoD (navy - gendarmerie maritime) -Ministry of Transport (Admin. Of Mar. Affairs)	-Ministry of budget (Customs) -Ministry of Interior (gendarmerie) - MoD (navy - gendarmerie maritime) -Ministry of Transport (Admin. Of Mar. Affairs)	MoD - French Navy

GERMANY

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Federal Ministry of Transport, Building and Urban Affairs/ Federal Waterways and Shipping Administration(2)/ Federal Ministry of Interior and Coastal States/ Federal Ministry of Transport, Building and Urban Affairs/ Federal Ministry of Defense(3), German Navy/	*Within Territorial Waters:* Ministries of the Coastal States/ Fishery Control Agencies of the Coastal States, partially Water Police (Schleswig-Holstein) *Outside Territorial Waters:* Federal Ministry of Food, Agriculture and Consumer	*Within Territorial Waters and Shore Areas:* Ministries of Environment of the Coastal States *Outside Territorial Waters:* Federal Ministry of Transport, Building and Urban Affairs/ Federal Waterways and Shipping Administration and CCME/ Environmental Authorities of the	Federal Ministry of Finance/ Federal Customs Administration/ Water Customs Service	Federal Ministry of Interior/ Federal Police	by each responsible Ministry/ by each responsible Authority - mainly Federal Waterways and Shipping Administration in close co-operation with Water Police of Coastal States	MoD - German Navy(3)

Federal Police and Water Police/ German Lifeboat Association *In case of a complex emergency situation:* CCME	Protection/ Federal Agency for Agriculture and Food	Coastal States				

(1) Network German Coastguard: The command centres of the Federation and the Coastal States including the Maritime Emergencies Reporting and Assessment Centre of the Central Command for Maritime Emergency (CCME) are operating together in the Joint Emergency Reporting and Assessment Centre under the roof of the German Maritime Safety and Security Centre in Cuxhaven. Each agency retains the same responsibility in terms of geographical area and tasks as before, but information exchange, co-operation, co-ordination of operational means and support are optimized. In case of emergency situations the authority competent in the case will lead operations.

(2) also the Federal Maritime and Hydrographic Agency and See-Berufsgenossenschaft

(3) The German Armed Forces have the task to provide national security and defense against any threat from outside enemies. In accordance with a recent Supreme Court ruling concerning the Aviation Security Act, protection against imminent terrorist attacks may be considered as grave threats to security and the Armed Forces may act to prevent such threats in accordance with the German Constitution (Art. 35). In particular it is the task of the German Armed Forces to monitor all German Air and Water Space and to support other agencies in exercising sovereign rights. Rescue operations, evacuation operations and surveillance missions are also within the scope of tasks of the German Armed Forces

GREECE

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Ministry of Shipping, Maritime Affairs & The Aegean - Hellenic Coast Guard/ Ministry of Citizen's Protection-Civil Emergency/ Planning and Defence Directorate/ Ministry of Defence - Hellenic Navy and Air Force (when needed)	Ministry of Shipping, Maritime Affairs & The Aegean - Hellenic Coast Guard	Ministry of Shipping, Maririme Affairs & The Aegean - Hellenic Coast Guard	Ministry of Finance - Customs	Ministry of Sipping, Maririme Affairs & The Aegean - Hellenic Coast Guard (maritime borders) - Hellenic Police (land - air borders + reception and asylum processing)/ Ministry of Defence - Hellenic Navy (when needed)	Ministry of Shipping, Maririme Affairs & The Aegean - Hellenic Coast Guard	*Policy:* MoD *Operational:* Hellenic Navy

(1) on matters relating to the reception of migrants and granting of asylum

ICELAND

Maritime safety	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Ministry of the Interior, Icelandic Maritime Administration, Maritime Traffic Center, The Icelandic Coast Guard.	*Ministry of Fisheries and Agriculture, Directorate of Fisheries, The Icelandic Coast Guard.*	*Ministry for the Environment, The Environment Agency of Iceland, The Icelandic Coast Guard and the Maritime Administration.*	*Ministry of Finance, Directorate of Customs, The Icelandic Coast Guard, The Icelandic Police and The National Commissioner of Police.*	*Ministry of the Interior, The National Commissioner of Police, The Icelandic Police and The Icelandic Coast Guard.*	*Ministry of the Interior, The National Commissioner of Police and the Icelandic Coast Guard.*	*Ministry for Foreign Affairs, The Icelandic Coast Guard and The National Commissioner of Police.*

IRELAND

Maritime safety	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Policy Dept. of Transport *Operational* Irish Maritime Administration/ Irish Coast Guard/ National port Authorities/ Irish Defence Forces/ Voluntary SAR services	*Policy* Dept. of Agriculture, Food and The Marine *Operational* Sea Fisheries Protection Authority/ Irish Defence Forces	*Policy* Dept of Transport/ Dept of Environment *Operational* Irish Coast Guard/ Environmental Protection Agency	*Policy* Revenue Commissioners/ Dept of Justice, Equality and Law Reform. *Operational* Irish Police	*Policy* Dept of Defence/ Dept of Justice, Equality and Law Reform. *Operational* Irish Defence Forces/ Irish Police	*Policy* Dept of Justice, Equality and Law Reform/ Dept of Defence *Operational* Irish Police/ Irish Defence Forces	Policy: Dept.of Defence Operational: Navy

(1) Elements of Maritime Safety Policy function may be shared with the Department of Agriculture, Marine & Food if the Irish Coast Guard transfers from the Department of Transport Tourism and Sport.

(2) Policy function of Department of Transport, Tourism and Sport will move to the Department of Agriculture, Marine & Food if the Irish Coast Guard transfers

(3) The Irish Police are called An Garda Siochana

ITALY

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Ministry of Transport - Coast Guard/ State Civil Defence Department/ Sea Emergency Operations Centre(1)	Ministry of Agricultural Policies/ Coast Guard (National Fishing Control Centre)/ Navy	Ministry of Environment, Territory and Sea/ Ministry of Transport - Coast Guard	Ministry of Economy and Finance - Customs	(3) Ministry of Interiors - Police Forces/ Ministry of Transport - Italian Coast Guard(2)/ Ministry of Defence - Navy/ Ministry of Economy and Finance - Customs	(4) Ministry of Transport - Coast Guard/ Ministry of Interiors - Police Forces/ Ministry of Defence - Navy	*Policy:* MoD *Operational:* Navy

(1) manned with personnel of the Coast Guard

(2) when a SAR operation is also needed

(3) Italian Institutions who work in the field of Border Control operate under coordination of the Ministry of the Interior.

(4) if "Law Enforcements" has to be considered in a broader way (since authorities different from real Police Forces have been included, e.g. Coast Guard and Navy), other authorities like Ministry of Economy and Finance shall be added. In any case, the

LATVIA

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Ministry of Transport - Maritime Administration/ Ministry of Defence - Coast Guard/ Harbour Master Offices/ Ministry of Environment	Ministry of Agriculture - National Board of Fisheries/ Marine and Inland Waters Administration	Ministry of Environment - Marine and Inland Waters Administration/ Ministry of Defence - Coast Guard/ Port Authorities	Ministry of Finance - Customs	Ministry of Interior/ State Border Guard	-Security Police -State Police -Municipal Police	*Policy:* MoD *Operational:* Navy

LITHUANIA

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Ministry of Transport and Communications/ Lithuanian Maritime Safety Authority/ Klaipeda State Seaport Authority/ Maritime and Aviation Rescue Centres(1)	-Ministry of Agriculture - Fisheries Service -Navy/Joint Military Commite	Ministry of Transport and Communications/ Ministry of Environment/ Lithuanian Maritime Safety Administration/ Klaipeda Regional Environmental Protection Department/ Maritime Rescue Centre (Naval Force (Ministry of National Defence))	Ministry of Finance - Customs Department	Ministry of the Interior/ State Border Guard Service	Ministry of the Interior - Police Department/ Ministry of the Interior - State Border Guard Service	Ministry of National Defence - Naval Force

91

(1) composed by the Naval Force (Ministry of National Defence) and the Civil Aviation Administration

MALTA						
Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Malta Maritime Authority/ Ministry of Transport and Communications/ Armed Forces of Malta/ Civil Protection Department	Ministry of Rural Affairs and Environment - Fisheries Conservation & Control Division	Malta Maritime Authority/ Ministry of Rural Affairs and Environment (1)/ Oil Pollution Response Module (OPRM)/ Civil Protection Department	Ministry of Finance/ Customs Dept	Armed Forces of Malta/ Police	Police	Armed Forces of Malta

(1) Malta Environment & Planning Authority has a monitoring role

NORWAY						
Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Policy: Ministry of Fisheries and Coastal Affairs/ Ministry of Defence/ Ministry of Justice and the Police/ Ministry of Trade and Industry *Operational*: Coastal Administration/ Coast Guard/ Armed Forces/ Police/	*Policy*: Ministry of Fisheries and Coastal Affairs *Operational*: Directorate of Fisheries/Coast Guard	*Policy*: Ministry of Fisheries and Coastal Affairs/ Ministry of the Environment *Operational*: Norwegian Coastal Administration/ Coast Guard/ Norwegian Radiation Protection Authority/ Climate and Pollution Agency	*Policy*: Ministry of Finance *Operational*: Customs/ Coast Guard	*Policy*: Ministry of Justice and the Police *Operational*: Police/ Customs/ Coast Guard	*Policy*: Ministry of Justice and the Police *Operational*: Police/ Coast Guard	*Policy:* Ministry of Defence *Operational:* Armed Forces/ Coast Guard

JRCC/ Norwegian Maritime Directorate/ Customs						

<div style="background-color: yellow">

NETHERLANDS (1)

</div>

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Ministry of Transport, Public Works and Water Management (2) - North sea Dept/ Coastguard(3)/ Regional Authorities(4)/ Port Authorities/ Shipping Inspectorate(5)/ MoD - Royal NL Navy/ Royal Netherlands Lifeboat Institution/ Ministry of Economic Affairs(6)	-Ministry of Agriculture, Nature and Food Quality General Inspection Administration (nVWA) - Coastguard/ Maritime Police	Ministry of Transport, Public Works and Water Management(2) - North sea Dept/ Coastguard	Ministry of Finance - Customs/ Coastguard	Justice - Public Prosecutor + Royal Military Constabulary/ Coastguard(7)	Ministry of Justice - Public Prosecutor/ enforcement services/ Coastguard(7)/ National Police Service Agency	MoD(8) - Royal Netherlands Navy

(1) Policy cooperation and integration through the Coordinating Minister for North Sea Affairs (= Minister of Transport etc.) and the Inter-ministerial Board of North Sea Directors. Integrated North Sea policy established in the General Policy Paper on Sp

(2) In case of a substantive accident/disaster a representative of the ministry of Transport, Public Works and Water Management chairs an inter-ministerial policy-team in order to ste team at the Coastguard Centre

(3) The Netherlands' Coastguard is a cooperative framework under the operational coordination and command of the Royal Netherlands Navy, bundling the majority of governmental operational services and (civil and military) resources into one functional orga

(4) Regional authorities are responsible for vessel traffic management in the approaches and entrances to the Netherlands' seaports, including the provision of pilotage and vessel traffic services

(5) The Shipping Inspectorate is part of the Transport and Water Management Inspectorate of the ministry of Transport, Public works and Water Management

(6) The Ministry of Economic Affairs is responsible for offshore exploration of oil and gas, wind-farming, cables and pipes, (coastal) tourism

(7) Operational cooperation and integration through the Netherlands Coastguard, under the operational coordination and command of the Royal Netherlands Navy.

Integrated operational framework established in annual Coastguard plans and programmes

(8) The ministry of Defence is responsible for military uses of the sea, including military exercising, and is operationally responsible for the Netherlands Coastguard and the Hydrographical Service

POLAND

Maritime safety, security etc.	Fisheries control	Pollution response	Customs	Border control	Law Enforcement	Defence
Maritime Security (1): Ministries of: Infrastructure, Interior and Administration, National Defense, Finance, Foreign Affairs. Maritime Offices, SAR Service (2), Border Guard, Police, State Fire Brigades (3) and Customs Service (4) and Navy (5) **Maritime Safety:** Ministry of Infrastructure, Maritime Offices, SAR Service and Border Guard	Ministry of Agriculture and Rural Development, Regional Sea Fishery Inspectorates, Agricultural and Food Quality Inspection, Veterinary Inspection (6) in cooperation with Border Guard, Police and Customs Service	Maritime Offices in cooperation with SAR Service and Border Guard Marine environment protection: Chief Inspectorate for Environmental Protection (7)	Ministry of Finance in cooperation with Customs Service and Border Guard	Border Guard	by each responsible Ministry or Authority, in particular: Maritime Offices and Ministry of Infrastructure in cooperation with Border Guard, Police, Customs Service	Navy

Ministry of Infrastructure (and supervised authorities) and Polish Border Guard are the most important institutions responsible for matters of maritime surveillance in Poland.

1. In principle the relevant Ministries are dealing with issues related to maritime surveillance on policy level, supervised authorities or services on operational level;

2. Maritime Offices (Gdynia, Słupsk, Szczecin), SAP. Service (Maritime Search and Rescue Service) are under supervision of Ministry of Infrastructure, which is responsible for coordination of the maritime policy in Poland, including integration of maritime surveillance;

3. Border Guard, Police and State Fire Brigades Services are under supervision of Ministry of the Interior and Administration;

4. Customs Service is under supervision of Ministry of Finance (relevant Customs Chambers: Gdynia, Olsztyn, Szczecin);

5. Navy (Navy Command, Maritime Operations Centre, Hydrographic office of the Polish Navy) is under supervision of Ministry of National Defense,

6. Regional Sea Fishery Inspectorates, Agricultural and Food Quality Inspection and Veterinary Inspection are under supervision of Ministry of Agriculture and Rural Development, Polish Fisheries Monitoring Centre (FMC) is a unit within this Ministry;

7. Chief Inspectorate for Environmental Protection is under supervision of Ministry of the Environment.

PORTUGAL

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Ministry of National Defence/ National Maritime Authority/ Portuguese Navy+Air Force/ Ministry of Public Works, Transports and Communications	Ministry of Agriculture - Rural Development and Fisheries/ System of Supervision and Fishing Activity Control (SIFICAP)/ Ministry of National Defence - Portuguese Navy+Air Force/ National Maritime Authority/ Ministry of Home Affairs/ National Republican Gu	Ministry of National Defence -Portuguese Navy+Air Force/ National Maritime Authority	Ministry of Justice - Judiciary Police/ Ministry of Finance- Customs and Special Duties General Administration/ Ministry of Home Affairs/ Fiscal Brigades	Ministry of National Defence - Portuguese Navy/Air Force/ National Maritime Authority/ Ministry of Home Affairs - Aliens and Border Service	Ministry of National Defence- Portuguese Navy+Air Force/ National Maritime Authority/ Ministry of Home Affairs/ National Republican Guard/ Aliens and Border Service	Ministry of National Defence - Portuguese Navy/ Air Force

ROMANIA						
Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Ministry of Transport and Infrastructure trough Romanian Naval Authority(1), Maritime Ports Administrations of Costanta and Galati (ports security)/ Ministry of Administration and Interior - Romanian Border Police General Inspectorate(2)	Ministry of Agriculture and Rural Development - National Agency for Fishery and Aquaculture/ Ministry of Administration and Interior - Romanian Border Police General Inspectorate(2)	**For pollution response:** Ministry of Environment and Forests (land-based pollution) - Water Resources Management Department/ Ministry of Transport and Infrastructure - Romanian Naval Authority (ships' pollution)/ Ministry of Administration and Interior - General Inspectorate for Emergency Situation(3) **For Marine env.:** Ministry of Environment and Forests - Water Resources Management Department(4)/ Ministry of Education, Research, Youth and Sports(5)	Ministry of Public Finance, National Customs Authority (6)	Ministry of Administration and Interior - Romanian Border Police General Inspectorate(2)	Ministry of Transport and Infrastructure - Romanian Naval Authority(1)/ Ministry of Administration and Interior - Romanian Border Police General Inspectorate (2), General Inspectorate of Romanian Police - Naval Transport Police Department (7)	Ministry of National Defence - Romanian Naval Forces

(1) under the coordination of the Maritime Rescue Coordination Centre

(2) trough Border Police County Inspectorate of Constanţa

(3) trough Emergency Situation County Inspectorate of Constanţa

(4) trough Water Resources Management Department, National Institute for Marine Research and Development "Grigore Antipa"

(5) trough National Authority For Scientific Research, The National Institute for Research and Development of Marine Geology and Geoecology – GeoEcoMar and

Romanian Space Agency

(6) through Customs offices and county directions for tolls and customs operations (Constanţa and Galaţi)

(7) trough Maritime Transport Police Department of Constanţa

SLOVENIA

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Ministry of Transport - Slovenian Maritime Administration/ Port State Control/ Ministry of Interior - Police/ Ministry of Defence/ Administration for Civil Protection and Disaster Relief/ Ministry of the Environment and Spatial Planning/ Environmental Age	Ministry of Agriculture, Forestry and Food/ Inspectorate of the Republic of Slovenia for Agriculture, Forestry and Food/ Ministry of the Interior - Police/ Ministry of Transport - Slovenian Maritime Administration	Ministry of Transport - Slovenian Maritime Administration/ Ministry of Defence/ Administration for Civil Protection and Disaster Relief/ Ministry of the Environment and Spatial Planning - Environmental Agency	Ministry of Finance - Customs Administration	Ministry of Interior - Police	Police/ Customs/ Navy/ Slovenian Maritime Administration	*Policy:* MoD *Operational:* Navy

SPAIN

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Ministry of Defence (Navy), Ministry of Public Works and Transport (SASEMAR), Ministry of Interior (Guardia Civil), Ministry of Environment,	Ministry of Environment, Rural and Marine Affairs - fisheries, Ministry of Interior (Guardia Civil), Ministry of	Ministry of Public Works and Transport (1), Ministry of Environment, Rural and Marine Affairs - protection of the marine env., Ministry of	Ministry of Economy and Finance (Customs), Ministry of Interior (Guardia Civil), Ministry of Defence (Navy).	Ministry of Interior (Guardia Civil)	Ministry of Interior (Guardia Civil) Ministry of Defence (Navy), Minstry of Economy and Finance (Customs), Ministry of	*Policy:* Ministry of Defence *Operational:* Navy, Guardia

| Rural and Marine Affairs - protection of the marine env., Ministry of Economy and Finance (Customs), Coastal Autonomous Communities. | Defence (Navy), Coastal Autonomous Communities. | Interior (Guardia Civil), Ministry of Defence (Navy), Coastal Autonomous Communities. | | | Public Works and Transport (Merchant Marine). | Civil |

(1) Together with the Coastal Regions, competent for Spatial Planning. Maritime Directorate (Harbour Masters and SASEMAR) competent for marine pollution response.

SWEDEN

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Policy: Ministry of Enterprise, Energy and Communications/ Ministry of Defence *Operational*: Maritime Administration/ Coast Guard/ Police/ Armed Forces	*Policy*: Ministry of Agriculture *Operational*: Board of Fisheries/ Coast Guard	*Policy*: Ministry of Enterprise, Energy and Communications/ Ministry of Defence *Operational*: Environmental Protection Agency/ Coast Guard	*Policy*: Ministry of Finance *Operational*: Customs/ Coast Guard	*Policy*: Ministry of Justice *Operational*: Police/ Customs/ Coast Guard	*Policy*: Ministry of Justice *Operational*: Police/ Customs/ Coast Guard	*Policy:* MoD *Operational:* Swedish Navy

UNITED KINGDOM

Maritime safety, security etc.	Fisheries control	Pollution response & Marine env.	Customs	Border control	Law Enforcement	Defence
Policy: Department for Transport (DfT) *Operational:* Maritime and Coastguard Agency (MCA) (1)	Fisheries is a devolved matter in the UK. **England:** *Policy (and lead for UK)*	*Policy* Department for Transport (DfT), Department for Environment, Food and Rural Affairs (Defra).	*Policy* Her Majesty's Revenue and Customs (HMRC) *Operational* Border Force (Home	*Policy/Operational* Border Force (Home Office)	Law enforcement (policing) is a devolved matter in Scotland and Northern Ireland **England & Wales:** *Policy*	*Policy* Ministry of Defence (MoD) *Operational* Royal Navy

	Department for Environment, Food and Rural Affairs (Defra). *Operational* The MMO is the 'sole' Copmpetent Authority' for the UK where required under the legislation.Marine Management Organisation (MMO) and the Royal Navy (indirect but through MMO) **Scotland**: Marine Scotland **Northern Ireland**: DARD and Sea Fisheries Inspectorate **Wales**; Welsh Assembly Government	*Operational* Maritime and Coastguard Agency (MCA) (1) Marine Management Organisation (MMO)	Office)	Home Office *Operational* National Crime Agency,Police **Scotland & Northern Ireland:** policing is a devolved matter

(1) in conjunction with government emergency planning

Note (February 2014): The information contained in this spreadsheet regarding responsibilities of UK Government Departments and Agencies and their data systems is based on an informal survey of contacts and may not be comprehensive. The National Maritime Information Centre (NMIC) acts as a data sharing hub for most of these Government Departments and Agencies.

11.   ANNEX 4: CONNECTION WITH OTHER EU POLICIES RELATED TO EGOVERNMENT

The CISE initiative operates within a larger framework of EU-level policies and strategies on eGovernment that have been developed in recent years. It is influenced by a number of EU policies and initiatives that need to be taken into consideration:

The Malmö Declaration[98]

The Malmö Declaration (Nov 2009) responds to the citizens' need for more open, flexible and user centric public services. The declaration points out that, in order to move towards a globally leading knowledge economy, a true Single Market with seamless eGovernment services and efficient and effective public administrations are key. Therefore remaining barriers to cross-border activity should be addressed and technical and legal pre-conditions and key enablers should be put in place. Furthermore, public administrations should re-design their administrative processes to reduce administrative burden. Member States (through the ministers in charge of eGovernment policy) committed to improve the conditions for interoperability of public administrations, to increase the positive effect of electronic collaboration on the delivery of public services.

The Granada Declaration[99]

The Granada Declaration complements the Malmö Declaration on eGovernment by encouraging the development of more efficient interoperable public services that promotes the re-use of public sector information, increase the efficiency of government and lead to a measurable reduction in administrative burdens on citizens and businesses as well as contribute to a low-carbon economy.

Europe 2020[100]

The Europe 2020 agenda proposes an ambitious strategy for Europe to exit from the economic crisis. Looking beyond the short term it aims for a smart, sustainable and inclusive future economy, realised by a collective European approach focusing on five key areas:

Employment: Modernising labour markets and empowering people by lifelong skills improvement.

Innovation: Improving framework conditions and access to finance for research and innovation.

Education: Enhancing the performance of education and reducing early school-leaving.

Social Inclusion: Ensuring social and territorial cohesion for every citizen to benefit from growth and jobs.

---

[98] http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf
[99] http://ec.europa.eu/ceskarepublika/pdf/press/ks7rada.pdf
[100] http://ec.europa.eu/europe2020/index_en.htm

Climate/Energy: Shiftingll towards a low carbon economy by increasing resource efficiency and modernising the transport sector.

These five key areas are defining concrete targets and are in turn broken down into seven flagship initiatives:

Innovation Union

Youth on the move

A digital agenda for Europe

Resource efficient Europe

An industrial policy for the globalisation era

An agenda for new skills and jobs

European platform against poverty

Efficient and effective public services, which the CISE initiative contributes to, contribute to the competitiveness of the EU economy.

Digital Agenda for Europe[101]

The Digital Agenda for Europe is one of the seven flagship initiatives of the Europe 2020 Strategy. It defines how wider deployment and more effective use of digital technologies will enable the delivery of the social and economic benefits Europe 2020 aims for. It follows the i2010, eEurope 2005, eEurope 2002 and eEurope initiatives. The Digital Agenda contains 101 actions and addresses seven main topics of improvement (called Pillars), one of them being **Interoperability:**

Pillar I - Digital Single Market: Regulatory limitations should be eliminated to facilitate cross-border use of commercial and cultural digital content and services and to enable citizens and businesses to fully benefit from the European Single Market.

Pillar II – Interoperability & Standards: Standardisation, public procurement and coordination between public authorities will improve the interoperability of digital services and devices.

Pillar III - Trust and Security: Responsive mechanisms and cooperation networks should be developed to address cyber-crime and to protect citizens' personal data and privacy.

Pillar IV - Very Fast Internet: To ensure the roll-out and take-up of broadband throughout Europe, investments in fast internet should be stimulated.

---

[101] Digital Agenda for Europe. http://ec.europa.eu/digital-agenda/ and Communication from the Commission to the Council, the European Parliament, the European economic and social Committee the Committee of the regions: "A Digital Agenda for Europe" COM(2010) 245 final/2 – 26.08.2010

Pillar V - Research and Innovation: Research and Innovation efforts should be stimulated by leveraging more private investment, improving coordination and increasing the opportunities for SMEs.

Pillar VI - Enhancing e-Skills: To decrease the professional IT skills shortage and to increase Europe's productivity, all European citizens should have a minimum level of digital literacy and skills.

Pillar VII - IT for Societal challenges: By smart use of IT societal challenges such as climate change, the ageing society, energy consumption and social exclusion can be addressed more effectively.

The Digital Agenda states that interoperability has the potential to contribute to the European economy's smart, sustainable and inclusive growth. This requires public services to flow across borders and across sectors, with electronic services and devices working together efficiently, based on common standards and open platforms.

The CISE initiative contributes to the realisation of the Digital Agenda for Europe. Seamless cross-domain and cross-border information exchanges are a priority for the EU, as is clearly indicated by the actions in the Pillar VII (*IT-enabled benefits for EU society*) and others of the Digital Agenda. The CISE initiative facilitates

Pillar I - *Digital Single Market,* e.g. action 3 on opening up public data for re-use by other public authorities).

Pillar II - *improving standard-setting procedures and increased interoperability,* namely action 27 under which Member States should implement commitments on interoperability and standards in the Malmö and Granada Declarations by 2013. Action 23 is the "umbrella" action for the Interoperability and Standards Pillar of the Digital Agenda.

Pillar VII for *IT-enabled benefits for EU society*. CISE contributes to action 84 (*'Support seamless cross-border eGovernment services in the single market through the Competitiveness and Innovation Programme (CIP) and Interoperability Solutions for European Public Administrations (ISA) Programme'*) through its contribution to the ISA programme and action 89 (*'Member States should make eGovernment services fully interoperable overcoming organisational, technical or semantic barriers and supporting IPv6'*).

European eGovernment Action Plan 2011-2015[102]

The European eGovernment Action Plan 2011-2015, launched in December 2010, is the second eGovernment Action Plan commissioned by the European Commission and aims to realise the four goals set in the Malmö declaration (Empowerment of citizens and businesses; Mobility in the Single market; Efficiency and Effectiveness; Legal and technical pre-conditions). The plan is focused on using public resources more efficiently, reducing public expenditure and at the same time providing seamless eGovernment services that answer to the user's needs. In other words: Better public services with fewer resources.

---

[102] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:PDF

The eGovernment Action Plan sets three main targets (also based on the Digital Agenda):

By 2015, a number of key cross-border services will be available online

By 2015, 50% of EU citizens will have used eGovernment services

By 2015, 80% of enterprises will have used eGovernment services

The above three targets are to be achieved by stimulating joint action on eGovernment within Europe and by establishing the pre-conditions for eGovernment services development, such as **interoperability**, e-Signature and e-Identification.

Eventually the eGovernment Action Plan 2011-2015 should lead to more open, innovative and responsive public services, engaging, enabling and empowering citizens to use digital services. It will smoothen access to public services across the EU.

The ISA programme[103]

The Interoperability Solutions for European Public Administrations Programme (ISA) aims to foster interoperability between public administrations by helping to establish common approaches that will make collaboration a lot easier. Sharing and reusing tools such as common platforms and common components, along with the sharing of services like common infrastructures, will also play a part by keeping costs down and reducing time to market.

The ISA programme is a key actor for the delivery of cross-sector and cross-border electronic collaboration as it consists of actions that contribute to the cross-border and cross-sector interoperability, sharing and reuse of common specifications, tools and services.

Focus on semantics ensures that the precise meaning of the information remains when exchanged across borders in different languages. The ISA programme supports development and sharing of assets and methodologies in the semantics domain via its SEMIC action Activities in the area of semantic interoperability provide the means for public administrations to work together on common vocabularies, definitions and classifications of information in the domains of justice, social affairs, research, economy, health and many others. The CISE initiative is benefiting from work done under this action, e.g. by applying the methodologies it developed.

The ministers emphasised respect for privacy and data protection, as trust and security are integral when creating services that rely on the electronic exchange of information. In this area called *Trusted Information Exchange*, ISA supports a variety of actions, one of them being the *Trusted Exchange Platform* that supports the secure exchange of documents between local governments, national parliaments, EU institutions, citizens and businesses. The CISE initiative has also been funded by the ISA programme as relevant action in this *Trusted Information Exchange* area.

---

[103] Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on establishing a programme on interoperability solutions for European public administrations (ISA) — OJ L 260, 03.10.2009, p. 11.

The European Interoperability Strategy (EIS)[104] and the European Interoperability Framework (EIF)[105] are defined as annexes of the Commission Communication on interoperability for European public services[106], where it is stated that

"*For public administrations, interoperability brings benefits such as cooperation. It facilitates the exchange, sharing and reuse of information, thus improving the delivery of European public services to citizens and business, reducing costs and preventing duplication of efforts*".

The European Interoperability Framework (EIF) promotes and supports the delivery of European public services by fostering cross-border and cross-sectoral interoperability. The Commission Communication stipulates that *the EIF should be taken into account when making decisions on European public services that support the implementation of EU policy initiatives*. The work done so far under the CISE initiative has been based on the EIF.

The EIF is maintained under the ISA programme, in close cooperation between the Member States and the Commission. They work together in the spirit of Article 170 of the Treaty on the Functioning of the European Union. Under this Article, to help achieve the objectives referred to in Article 26 concerning the internal market, the European Union should help establish and develop trans-European networks and promote the interconnection and interoperability of national networks as well as access to such networks.

The EIF contributes to the better functioning of the internal market by increasing interoperability. The same applies for the CISE initiative.

---

[104]　http://ec.europa.eu/isa/documents/isa_annex_i_eis_en.pdf
[105]　http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf
[106]　Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "Towards interoperability for European public services" (COM(2010) 744 final) – 16.12.2010